NOVA IMS Information Management School

MGI

Mestrado em Gestão da Informação

Master Program in Information Management

Tecnologias IoT na Segurança Industrial

Fábio Ferreira dos Santos

Dissertação apresentada como requisito parcial para obtenção do Grau de Mestre em Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão da Informação

Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

Tecnologias IoT na Segurança Industrial

por

Fábio Ferreira dos Santos

Dissertação apresentada como requisito parcial para obtenção do Grau de Mestre em Gestão de Informação, com especialização em Gestão de Sistemas e Tecnologias de Informação.

Orientador: Vítor Santos, Professor, Universidade Nova de Lisboa

Setembro, 2020

Tecnologias IoT na Segurança Industrial

Este documento foi gerado utilizando o processador (pdf)LaTeX, com base no template "novathesis" [1]. [1] https://github.com/joaomlourenco/novathesis

Agradecimentos

Aos meus pais, por terem sido um pilar fundamental durante todo o meu percurso académico.

Ao Miguel Beatriz e João Tavares, pelo contributo e apoio durante a componente curricular do Mestrado em Gestão de Informação.

Ao Bruno Domingues, Anderson Taschin, Henrique S. Mamede e António Jordão, pelos seus contributos que permitiram melhorar os resultados alcançados pela presente dissertação.

Ao Professor Dr. Vítor Santos, por ter aceite ser o orientador desta dissertação, pelo seu contributo, orientação e disponibilidade.

Aos professores da Universidade Nova de Lisboa, por todo o apoio e conhecimento que transmitiram durante o meu percurso académico.

A todos os meus colegas, amigos e familiares, que contribuíram direta ou indiretamente para a realização desta dissertação.

Resumo

A segurança e saúde dos trabalhadores a nível industrial caracteriza-se por uma área de grande importância para as entidades empresariais, não só pela existência de uma maior consciencialização para os perigos e riscos a que os trabalhadores se encontram expostos, mas também derivada de legislação rígida e coimas associadas a acidentes de trabalho.

Os avanços tecnológicos como a *Internet of Things*, podem traduzir-se em melhorias significativas das condições de segurança dos trabalhadores, procurando eliminar ou reduzir o risco proveniente de perigos existentes em contexto laboral.

Este documento aborda os passos que conduziram à elaboração de uma *framework* que possa ser adotada pelos vários setores da indústria, tendo o objetivo de auxiliar o levantamento das necessidades e consequente seleção de tecnologias *Internet of Things*, com o intuito de incrementar a segurança dos trabalhadores com recurso à utilização dessas mesmas tecnologias.

Inicialmente é introduzida a temática da segurança industrial, justificando a importância que esta possui para a indústria. Apresentam-se aspetos gerais relacionados com fatores de perigo e avaliação de risco, bem como potenciais controlos a aplicar. De seguida, é referido o conceito de *Internet of Things*, as diferentes componentes a si adstritas e a sua potencial relação com a segurança industrial.

Posteriormente enunciam-se os pressupostos que serviram de base à elaboração do artefacto, seguindo-se a descrição de cada um dos componentes e etapas que constituem a *framework*.

Por fim, faz-se referência à avaliação da *framework* por parte de especialistas e discussão dos resultados obtidos, concluindo-se a utilidade do artefacto como suporte à utilização da *Internet of Things* na segurança industrial.

Palavras-chave: *Internet of Things*; Tecnologias de informação; Sistemas de informação; Segurança e higiene no trabalho; Segurança industrial

Abstract

The safety and health of workers in industrial workplaces is extremely important for companies, not only due to the awareness of the dangers and risks to which workers are exposed, but also promoted by strict legislation and existing penalties for occupational accidents.

Major technological advances, such as Internet of Things, can introduce significant improvements of working conditions in order to eliminate or reduce workplace hazards and risks.

This document addresses all steps that led to the elaboration of a framework which can be adopted by multiple industry sectors to conduct a survey on occupational health needs and select technologies that can increase the overall workplace safety.

Initially, the subject industrial safety and its importance is introduced. Aspects related with hazard factors and risk assessments are presented, as well as potential controls to apply. Then, the concept of Internet of Things is described as its components and presented the relation with industrial safety.

Subsequently, assumptions are presented and also a detailed description of each component and step of the framework.

Finally, a reference is made to the evaluation of the framework conducted by specialists and the results obtained from the discussion, concluding the usefulness of the artefact as a support for applying Internet of Things technologies in industrial safety.

Keywords: Internet of Things; Information technologies; Information systems; Occupational health and safety; Industrial safety

Índice

Lista de Figuras

Lista de Tabelas

Siglas

API *Application Programming Interface*

BLE *Bluetooth Low Energy*

DNS-SD *DNS Service Discovery*

EPC *Electronic Product Code*

GNSS *Global Navigation Satellite System*

GSM *Global System for Mobile Communications*

IEC *International Electrotechnical Commission*

IEEE *Institute of Electrical and Electronics Engineers*

IoT *Internet Of Things*

IPsec *Internet Protocol Security*

ISO *International Organization for Standardization*

LoRaWAN *Long-Range Wide-Area Network*

LTE *Long Term Evolution*

mDNS *Multicast DNS*

MQTT *Message Queue Telemetry Transport*

NFC *Near-Field Communication*

OSHA *Occupational Safety and Health Administration*

RFID *Radio-frequency Identification*

SenML *Media Types for Sensor Markup Language*

SensorML *Sensor Model Language*

TLS *Transport Layer Security*

UHF *Ultra High Frequency*

UPnP *Universal Plug and Play*

URI *Uniform Resource Identifier*

UWB *Ultra-Wide Bandwidth*

XMPP *Extensible Messaging and Presence Protocol*

Capítulo 1

Introdução

Com início no século XVIII (Britannica, 2019), em Inglaterra, a grande indústria moderna tem vindo a desenvolver-se de modo a acompanhar o crescimento da população mundial e procurando dar resposta às suas necessidades. Esse crescimento aliado ao domínio de novas técnicas, tecnologias e instrumentos de produção, contribuíram para incrementar a complexidade de processos de fabrico e conduzir a um aumento do número de atores envolvidos.

As diversas revoluções industriais que ocorreram ao longo da história da humanidade têm sido naturalmente acompanhadas por uma recorrente revisão de normas e procedimentos legais de segurança, tendo em vista garantir a segurança de todos os intervenientes em contexto laboral e visando a responsabilização das organizações pela sua falta de cumprimento.

Em resposta aos inúmeros riscos e ameaças à segurança e saúde dos trabalhadores, as empresas vêem-se obrigadas a desenvolver programas de segurança industrial que estejam de acordo com a legislação vigente em cada país. No entanto, a implementação destes programas não é suficiente para evitar a ocorrência de acidentes e a perda de vidas humanas, uma vez que a falha humana poderá estar naturalmente presente em múltiplos momentos.

Apesar dos esforços das organizações para assegurar o cumprimento dos protocolos e medidas de segurança, entre os anos de 2017 e 2018, a entidade americana *Occupational Safety and Health Administration* (OSHA) detetou cerca de 32 mil violações de diretrizes de segurança para os diferentes tipos de trabalho existentes na sociedade americana. Grande parte destas violações encontra-se relacionada com a ausência de equipamentos de proteção de quedas (7,720), sinalização de perigos (4,552), proteção de vias respiratórias (3,118) e procedimentos de *lockout/tagout*[1] de máquinas (2,944)

[1] Bloqueio e desbloqueio de máquinas para permitir p. ex. operações de manutenção enquanto os

(OH&S, 2018).

Recentemente, com o desenvolvimento da Internet e o surgimento de sensores de dimensões reduzidas, a par da sua introdução a nível industrial, surgiu o termo indústria 4.0 – considerada por muitos como sendo a 4ª revolução industrial. Por indústria 4.0 pressupõe-se a existência de um ambiente industrial onde o meio virtual e físico se fundem, fomentando entre si uma elevada cooperação que pode ser observada a diversos níveis (Schwab, 2016).

Um dos pilares da indústria 4.0 assenta na *Internet Of Things* (IoT) que permite a utilização de múltiplos dispositivos ligados entre si para um número ínfimo de potenciais aplicações, desde a monitorização e gestão de energia, até a veículos interligados com o intuito de antecipar e reduzir o risco de colisões (Wold Economic Forum, 2019).

1.1 Contexto e enquadramento

A segurança e saúde a nível industrial assume-se atualmente como uma área de enorme importância para as empresas, não só pelo facto de existir uma maior consciencialização adstrita aos perigos e ameaças a que os trabalhadores se encontram expostos, mas também fruto da existência de legislação rígida e coimas pesadas para as entidades que não garantirem a saúde e segurança dos seus trabalhadores aquando do desempenho de tarefas laborais (OSHA Education Center, 2018).

É neste contexto que surge a oportunidade de aliar as inovações tecnológicas, como a IoT, a processos que carecem de algum grau de informatização, procurando eliminar ou reduzir o risco proveniente dos perigos existentes em contexto laboral. Por exemplo, uma potencial fonte de perigos advém da execução de procedimentos de *lockout/tagout* que envolvem o correto isolamento das diferentes fontes de energia de um dado equipamento (OSHA, 2019). Por fonte de energia deduz-se fontes elétricas, hidráulicas, mecânicas, pneumáticas, químicas, térmicas, entre outras.

De notar ainda que onde ocorrem intervenções de manutenção, como as próprias características do trabalho, podem configurar numa necessidade efetiva da utilização de equipamentos de proteção individual específicos ou na presença de sistemas que detetem cenários anómalos (p. ex. presença inesperada de gases tóxicos). Por vezes, esses requisitos são variáveis e dependem de condições momentâneas.

Num contexto de necessidade e considerando a inovação tecnológica das últimas décadas, a IoT tem vindo a assumir-se como uma tecnologia apropriada ao controlo e gestão em ambiente industrial, promovendo a criação de fábricas inteligentes. A integração de sensores em ferramentas e equipamentos, a par da utilização de óculos com tecnologia de realidade aumentada que permitiu aos trabalhadores da Airbus, por exemplo, reduzir a ocorrência de erros humanos e melhorar significativamente a sua

equipamentos encontram-se desligados e as fontes de energia isoladas.

produtividade (Derber, 2018), são alguns exemplos do potencial intrínseco da adoção de novas tecnologias.

1.2 Motivação

A atividade industrial e a promoção da saúde e segurança dos trabalhadores, revelam um espectro considerável de oportunidades para o desenvolvimento de novas soluções.

A garantia da correta seleção de equipamentos de proteção individual de acordo com as tarefas e as condições atuais do meio envolvente, é apenas uma das necessidades que podem ser encontradas em contexto laboral e que pode conduzir à minimização de potenciais fontes de perigo através do cruzamento de informação em tempo-real.

A IoT e as suas características traduzem-se numa oportunidade para promover a segurança industrial. A seleção adequada de soluções IoT por parte das organizações poderá provocar um impacto positivo não só nos níveis de produtividade mas também do ponto de vista da segurança e saúde no trabalho.

1.3 Objetivos

O objetivo desta dissertação é o desenvolvimento de uma *framework* que possa ser utilizado pela indústria, auxiliando a identificação de necessidades e consequente seleção de tecnologias IoT, de modo a melhorar a segurança dos trabalhadores com recurso à utilização dessas tecnologias. Neste contexto, procura-se responder à questão:

- Será possível criar uma *framework* que possa ser adotada pelos vários setores da indústria, tendo em vista o apoio na seleção de tecnologias IoT que incrementem a segurança dos trabalhadores em contexto laboral?

Para alcançar o referido objetivo, serão considerados os seguintes objetivos secundários:

- Estudo da segurança e saúde no trabalho em âmbito industrial;
- Identificação dos principais perigos associados a máquinas e processos industriais;
- Identificação de tecnologias IoT que possam contribuir para a melhoria das condições de segurança dos trabalhadores.

1.4 Estrutura do documento

Em adição a este capítulo, o presente documento encontra-se estruturado da seguinte forma:

- Capítulo 2 – *Revisão de literatura*. Aborda a saúde e segurança em contexto industrial, detalha a IoT e demonstra a possível relação entre ambas as temáticas.
- Capítulo 3 – *Metodologia*. Enuncia a metodologia adotada e a estratégia de investigação utilizada na elaboração da presente dissertação.
- Capítulo 4 – *Framework para seleção de tecnologias IoT*. Apresenta a *framework* desenvolvida no âmbito da dissertação. Refere a avaliação do artefacto realizada por especialistas e a discussão dos resultados obtidos.
- Capítulo 5 – *Conclusão*. Versa sobre as conclusões e faz referência ao trabalho que poderá vir a ser desenvolvido futuramente.

Capítulo 2

Revisão de literatura

Este capítulo introduz a temática da segurança industrial, detalha a IoT e demonstra algumas das suas aplicações na promoção da saúde e segurança dos trabalhadores.

2.1 Segurança industrial

A saúde e segurança no trabalho é uma área que se concentra na promoção, desenvolvimento e manutenção do ambiente laboral, nomeadamente ao nível da execução de programas e políticas que garantam o bem-estar físico, mental e emocional dos trabalhadores. Procura ainda fomentar um ambiente de trabalho livre de quaisquer riscos (atuais ou potenciais) que possam afetar negativamente os trabalhadores (DIMULESCU e DOBROTĂ, 2018 Nyirendaavwil et al., 2015).

Apesar de existirem relatos esporádicos ao longo da história da humanidade em relação a problemas de saúde ou acidentes provocados pela atividade laboral, só a partir da revolução industrial é que a segurança e saúde no trabalho assumiu especial relevância.

Atualmente, a ILO, 2019, estima que o número anual de mortes provocadas por acidentes ou doenças relacionadas com trabalho ascenda a cerca de 2,3 milhões; o que corresponde a mais de 6 mil mortes diárias. A estatística resulta do registo anual de cerca de 340 milhões de acidentes de trabalho em todo o mundo.

A ocorrência de incidentes é algo transversal a todos os setores da indústria, pese embora o facto de alguns setores poderem apresentar mais ameaças do que outros para a saúde e segurança dos trabalhadores.

Determinar qual é a indústria mais perigosa depende diretamente da métrica utilizada para efetuar essa avaliação (p. ex. número total de mortes vs. taxa de lesões não-fatais por determinado número de trabalhadores). Contudo, independentemente

da métrica utilizada, em 2018, concluiu-se que alguns dos setores mais perigosos da indústria americana são (Injury Facts, 2018):

- **Construção:** Maior número total de mortes.
- **Agricultura e Pesca:** Maior taxa de mortes por 100 mil trabalhadores.
- **Transporte e Armazenamento:** Maior taxa de lesões não-mortais ou doenças em relação a dias de ausência do trabalho, por cada 10 mil trabalhadores.

A dimensão das empresas pode ter um impacto significativo na quantidade de acidentes laborais. Por exemplo, é notória a existência de um rácio superior de acidentes em pequenas e médias empresas quando comparado com organizações de maiores dimensões. Os motivos para estas diferenças podem estar relacionados com a falta de recursos em termos financeiros, humanos ou tecnológicos. Em alguns casos, a ausência de recursos é atribuída apenas a constrangimentos financeiros e obriga a que as responsabilidades inerentes à gestão da segurança e saúde no trabalho sejam delegadas a recursos humanos que podem não ter a formação ou experiência adequada (Nyirendaavwil et al., 2015).

No entanto, independentemente da dimensão das organizações, as grandes dificuldades encontradas pelas empresas na garantia das condições de segurança laborais podem derivar de (Nyirendaavwil et al., 2015):

- Ausência de recursos humanos, financeiros ou tempo;
- Perceção deficiente de legislação, políticas de segurança e identificação de riscos;
- Falta de formação na área de gestão da segurança e saúde no trabalho;
- Carência de suporte especializado ou auxílio na interpretação e implementação de políticas de segurança;
- Ausência de práticas que fomentem a existência de uma cultura de segurança;
- Escassez de sensibilidade para a temática da segurança e saúde no trabalho.

No que diz respeito às circunstâncias em que acontecem os acidentes de trabalho, estes tendem a ocorrer em vários momentos (Cheng et al., 2010):

- Durante o primeiro dia em que o trabalhador desempenha as suas tarefas;
- Utilização incorreta de equipamentos de proteção individual;
- Os equipamentos de proteção individual não são utilizados corretamente;
- Os trabalhadores não adotaram medidas de salvaguarda ou ignoraram os sinais de alerta de perigo;
- Gestão ineficiente da saúde e segurança dos trabalhadores em contexto laboral.

2.1.1 Fatores de perigo e avaliação de risco

Enquanto um perigo define-se como qualquer potencial fonte de danos ou efeitos adversos na saúde e bem-estar dos trabalhadores, um risco representa a probabilidade dos trabalhadores sofrerem o dano ou efeito resultante da exposição ao perigo (Canadian Centre of Occupational Health and Safety, 2020).

O impacto dos perigos na saúde dos trabalhadores depende de vários aspetos (IPIECA/OGP, 2006):

- Duração e níveis de exposição;
- Modo de exposição;
- Características do agente causal;
- Sensibilidade individual do trabalhador.

A Tabela 2.1 ilustra exemplos de cada uma dos diferentes grupos de fatores de perigo que podem ser encontrados em ambiente industrial. O conjunto de riscos varia naturalmente de acordo com a atividade e setor industrial em causa. Ou seja, enquanto um trabalhador da construção civil pode estar sujeito ao risco de queda, um pescador estará mais sujeito ao risco de afogamento.

De acordo com Vadimovna e Sergeevich, 2017, a minimização de riscos acontece numa ótica de mitigação ou prevenção. Em relação à mitigação de riscos, pode-se proceder à implementação de:

- Barreiras físicas;
- Sistemas anti-incêndio;
- Procedimentos de evacuação;
- Resposta adequada dos serviços de emergência.

De outro modo, a prevenção de riscos pode ocorrer através de:

- Identificação de todos os procedimentos e atividades que possam originar cenários de risco para os trabalhadores;
- Implementação de sistemas de controlo para a avaliação dos processos industriais;
- Instalação de sistemas de monitorização e alarme com o objetivo de detetar cenários anómalos numa fase precoce;
- Instalação de sistemas de controlo de segurança (p. ex. sistema automatizado para desligar uma máquina);

Natureza do perigo	Exemplos
Geográfica	- Temperatura ambiente e níveis humidade - Qualidade do ar - Variações térmicas - Infraestruturas de comunicação - Distância a cuidados de saúde - Espaços restritos / confinados - Trabalhos em altura
Física	- Fontes de ruído, vibração, pressão ou radiação - Níveis de iluminação ambiente - Objetos utilizados (p. ex. pontiagudos) - Meios de transporte
Química	- Libertação de poeiras, fibras, gases ou vapores - Contacto com ácidos
Biológica	- Doenças sexualmente transmissíveis - Comida ou bebida contaminada - Higiene deficiente - Epidemias
Ergonómica	- Postura incorreta - Transporte de carga sem meios adequados
Psicossocial	- Isolamento - Descriminação - Trabalho por turnos ou privação do sono - Volume de trabalho - Falta de comunicação

Tabela 2.1: Fatores de perigo (adaptado de IPIECA/OGP, 2006, Gardner, 2003, FESETE, 2010, Niven e McLeod, 2009)

- Adoção de mecanismos físicos de proteção (p. ex. válvulas para prevenir condições de pressão elevada).

Após a identificação dos perigos, a realização de avaliações de risco é um aspecto muito importante na medida em que é um processo sistemático para avaliar e classificar os riscos associados a determinados perigos (Rout e Sikdar, 2017). Habitualmente, a avaliação de riscos pode ter duas abordagens (Banaitiene e Banaitis, 2012):

- **Qualitativa:** Envolve a descrição de riscos e respetivos impactos ou a rotulagem subjetiva do risco em várias categorias (p. ex. alto, médio ou baixo) de acordo com a sua severidade e probabilidade de ocorrência. Facilita a prioritização de riscos para posterior análise ou mitigação direta. A Tabela 2.2 apresenta um exemplo de uma matriz de análise qualitativa.

- **Quantitativa:** Recorre a metodologias mais sofisticadas para a avaliação de risco, procurando estimar a frequência da sua ocorrência e determinar a magnitude das suas consequências (p. ex. com recurso a árvores de decisão).

Probabilidade de ocorrência	**Severidade**				
	Descartável	Reduzida	Moderada	Considerável	Catastrófica
Raro	Baixo	Baixo	Baixo	Moderado	Moderado
Improvável	Baixo	Moderado	Moderado	Alto	Alto
Moderado	Moderado	Moderado	Alto	Extremo	Extremo
Provável	Moderado	Alto	Extremo	Extremo	Extremo
Muito provável	Moderado	Alto	Extremo	Extremo	Extremo

Tabela 2.2: Exemplo de uma matriz de análise qualitativa (adaptado de Collins et al., 2014)

2.1.2 Controlo de perigos

A Figura 2.1 ilustra a hierarquia de controlos que visa determinar quais as medidas de segurança a adotar em relação aos perigos existentes na indústria. Manuele et al., 2008, define esta hierarquia como sendo uma forma sistemática de pensar e agir, em que as etapas se encontram classificadas numa ordem sequencial, de modo a escolher os meios mais eficazes para a eliminação ou redução de perigos, bem como dos riscos associados.

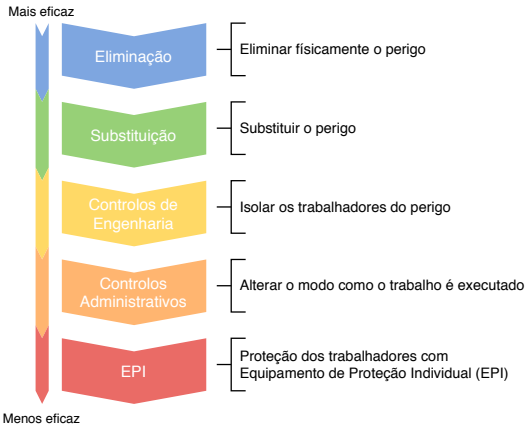


Figura 2.1: Hierarquia de controlos aplicados aos perigos (adaptado de CDC, 2015)

O topo da hierarquia é constituído por medidas proactivas no que diz respeito ao controlo de perigos, tornando-se por isso mais confiáveis e eficazes na promoção da segurança. Em oposição, os níveis inferiores são vistos como medidas reativas e por isso menos confiáveis. Esta hierarquia encontra-se dividida pelos seguintes níveis:

- **Eliminação e substituição de perigos:** São os controlos mais desejados por serem aqueles que representam um maior grau de eficácia na eliminação ou redução de riscos. O objetivo da substituição é de, por exemplo, utilizar substâncias com menor risco do que outras. Contudo, é importante garantir que o substituto não produz efeitos indesejados e prejudiciais, sendo por isso necessário controlar e monitorizar as exposições a eventuais novos perigos. A adoção destes controlos tende a ser mais difícil em processos já existentes, embora possa ser simples e apresentar baixos custos de implementação durante as fases de desenho e desenvolvimento de processos industriais (CDC, 2015, Topmiller e Dunn, 2013).

- **Controlos de engenharia:** Introdução de modificações em equipamentos, processos ou sistemas que reduzem o risco de exposição do trabalhador a um dado perigo. Operam numa ótica de isolamento do perigo, removendo a condição perigosa do local de trabalho (p. ex. através de um sistema de ventilação) ou instalando barreiras entre o trabalhador e o perigo (p. ex. proteções em máquinas de corte). Tratam-se de controlos que atuam ao nível da fonte ou transmissão do perigo, antecipando o momento de exposição. Podem funcionar continuamente e sem qualquer supervisão ou intervenção humana (Safeopedia, 2019b).

- **Controlos administrativos:** Implementação de políticas, regras e cronogramas que alteram a forma como as tarefas são executadas pelos trabalhadores. Definem procedimentos e padrões (p. ex. práticas de manutenção) para reduzir a exposição a perigos ou diminuir os riscos adstritos a tarefas que possam ser consideradas perigosas (Safeopedia, 2019a).

- **Equipamentos de proteção individual:** Equipamentos (p. ex. luvas, roupas de proteção, entre outros) que representam a última opção a ter em consideração para controlar a exposição dos trabalhadores a perigos. Utilizados quando os controlos de engenharia e administrativos não são viáveis ou eficazes para reduzir essa exposição a níveis aceitáveis; ou de utilização temporária consoante o cenário (Topmiller e Dunn, 2013).

2.2 *Internet of Things* (IoT)

Esta secção apresenta um breve estudo acerca da IoT, descreve conceitos e aborda as principais arquiteturas e tecnologias utilizadas.

2.2.1 Conceitos e características

Não existe uma definição única para a IoT, uma vez que os conceitos existentes revelam tendências de acordo com as características que cada um dos autores pretende enfatizar. Neste sentido, apresentam-se de seguida alguns conceitos que visam contribuir para uma melhor compreensão do que é a IoT.

Segundo duas organizações que se dedicam à definição de padrões internacionais na área das tecnologias da informação – *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC) –, a IoT caracteriza-se por:

> "Uma infraestrutura de objetos interconectados, pessoas, sistemas e recursos de informação que atuam em conjunto com serviços inteligentes para permitir processar informação do mundo físico e virtual, com o intuito de originar uma determinada reação." (ISO/IEC JTC 1, 2015)

A IoT também pode ser definida como uma rede de objetos físicos que têm tecnologia incorporada para permitir comunicação ou interação entre os seus estados internos e o ambiente externo (Gartner, 2019).

O *Institute of Electrical and Electronics Engineers* (IEEE) entende que um sistema IoT é formado por coisas "únicas" que podem ser identificadas através de identificadores globais únicos, acessíveis a partir de qualquer lugar e disponíveis a qualquer momento. O volume de informação fornecido por estas "coisas", a cada acesso efetuado, pode ser tão pequeno como, por exemplo, um identificador estático armazenado em etiquetas *Radio-frequency Identification* (RFID). Acrescenta ainda que uma das exigências para que um dado sistema seja considerado como uma IoT, assenta no pressuposto das referidas "coisas" encontrarem-se ligadas à Internet (Minerva et al., 2015).

Também é defendida a tese de que estas "coisas" são participantes ativos ao nível de processos sociais, de negócio e de informação, tendo a capacidade de interagir e comunicar entre si e com o meio ambiente, através da recolha de dados e informações percecionadas por sensores, enquanto reagem autonomamente a eventos do mundo físico/real e influenciando-o através da execução de ações e criação de serviços com ou sem intervenção humana (Sundmaeker et al., 2010).

Apesar da existência de múltiplos conceitos que procuram explanar a IoT, existem algumas caraterísticas que devem ser consideradas aquando do desenho e implementação de arquiteturas. Segundo Wang et al., 2017, estas características podem ser divididas em:

- **Interoperabilidade:** Permite a integração de diversos dispositivos, redes, sistemas e APIs, entre vários domínios e sistemas. Trata-se da capacidade de integração de dispositivos heterogéneos através, por exemplo, de *middlewares* inter-aplicacionais com o objetivo de fomentar a sua independência de plataformas e redes.

- **Orientação a serviços:** Possibilita a disponibilização e consumo de serviços independentemente das tecnologias ou produtos utilizados.
- **Modularidade e flexibilidade:** Favorece a separação lógica entre objetos e serviços, favorecendo a sua reutilização. As dimensões custo e tempo podem ser reduzidas através desta abordagem.
- **Comunicação multiponto:** Adota mecanismos para que múltiplos objetos possam comunicar entre si e em simultâneo. Por exemplo, a existência de um serviço que necessite de comunicar concorrentemente com múltiplos objetos, induz a necessidade de implementações *multithreading*.
- **Dinamismo e configuração em *runtime*:** Permite adicionar e remover objetos de redes e sistemas, de forma dinâmica e de acordo com as necessidades (p. ex. mover objetos entre redes). A tipologia de rede pode moldar-se e alocar mais recursos para suportar todos os objetos e serviços que se encontram ligados.
- **Descentralização e controlo de interação:** Suporta o acesso distribuído a dados, processamento e armazenamento. Permite definir que objetos devem ser passíveis de interação e restringir acessos para evitar ações inesperadas.
- **Facilidade de instalação:** Reduz custos adstritos à implementação e manutenção do sistema de IoT, favorecendo a existência de um modo *plug-n-play* em que novos dispositivos pré-programados têm que ser apenas ligados para entrarem em pleno funcionamento.

2.2.2 Arquitetura

A necessidade da IoT albergar um número ínfimo de dispositivos heterogéneos conduz à existência de várias arquiteturas possíveis que variam de acordo com o caso de estudo e respetivas necessidades. Deste modo, é fundamental que haja flexibilidade no número de camadas que fazem parte da arquitetura.

Enquanto o modelo mais básico assenta em 3 camadas – perceção, rede e aplicacional –, existem autores que sugerem um aumento desse número derivado da complexidade dos sistemas de IoT (Al-Fuqaha et al., 2015). A Figura 2.2 ilustra a comparação entre arquiteturas de 3 e 5 camadas, em que a primeira caracteriza-se por uma abstração da segunda, uma vez que a camada aplicacional engloba a de negócio, aplicacional e de *middleware*.

A arquitura de 5 camadas pode ser detalhada da seguinte forma (Khan et al., 2012):

- **Camada de perceção:** Composta por sensores que efetuam leituras do meio externo (p. ex. sensor de temperatura) e atuadores que realizam algum tipo de ação sobre o ambiente. Cada dispositivo que se encontra nesta camada tem um identificador único e os dados recolhidos pelos sensores são enviados para a camada de rede.

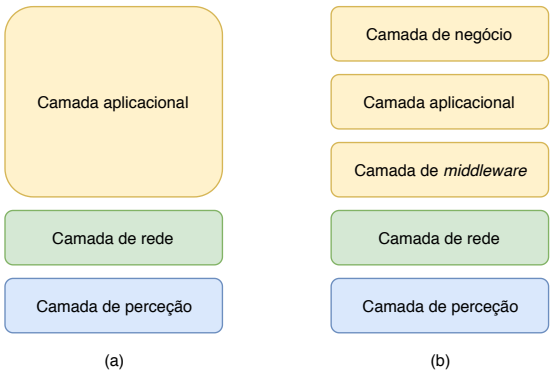


Figura 2.2: Arquitetura IoT de 3 (a) e 5 (b) camadas (adaptado de Khan et al., 2012 e Al-Fuqaha et al., 2015)

- **Camada de rede:** Representa os mecanismos e protocolos utilizados para transmissão de dados entre as camadas de perceção e de *middleware*.

- **Camada de *middleware*:** Responsável por gerir serviços, tomar decisões de acordo com os dados que são recebidos e gravá-los em bases de dados. Processa dados e toma ações automatizadas de acordo com os resultados. Esta camada permite ainda que dispositivos comuniquem entre si de acordo com o tipo de serviço implementado.

- **Camada aplicacional:** Fornece informação de acordo com os serviços requisitados por utilizadores finais. Esta camada molda-se ao contexto do caso de estudo.

- **Camada de negócio:** Versa sobre a monitorização de atividades e configurações do sistema de IoT. Constituída por ferramentas de construção de relatórios, gráficos, fluxogramas, entre outros, tendo por base a informação recebida da camada aplicacional. O resultado da sua análise poderá conduzir à definição de ações futuras e novas estratégias de negócio.

2.2.3 Tecnologias facilitadoras

As tecnologias que favorecem a IoT variam de acordo com o cenário e domínio do problema em estudo.

Numa situação em que haja a necessidade de rastrear a localização de veículos de transporte de mercadorias deve-se ter em consideração tecnologias e protocolos de comunicação que favoreçam a conexão de um elevado número de dispositivos móveis em simultâneo. No entanto, no caso da IoT ser empregue a nível hospitalar, o principal foco deve passar pela garantia da integridade e fiabilidade do sistema.

De seguida, descreve-se genericamente algumas das tecnologias que podem ser normalmente encontradas numa arquitetura de 5 camadas (apresentada na secção 2.2.2).

2.2.3.1 Tecnologias da camada de percepção

A camada de percepção é composta por dispositivos que podem ser classificados em 3 categorias (Li e Gan, 2013):

- **Passivos:** Dispositivos indicados para a comunicação unidirecional, que não possuem fonte de alimentação e podem depender de leitores externos para o fornecimento de energia (p. ex. energia eletromagnética). Exemplos: *QR codes*; códigos de barras; etiquetas RFID passivas.
- **Semi-passivos:** Dispositivos que possuem baterias que alimentam etiquetas enquanto recebem sinais de leitores. Favorecem um maior alcance e permitem a comunicação bidirecional. Exemplos: etiquetas RFID semi-passivas; leitores de infravermelhos.
- **Ativos:** Dispositivos com baterias de maiores dimensões e com uma área de alcance superior. Exemplos: atuadores inteligentes; dispositivos com sensores incorporados como giroscópio, monitorização de frequência cardíaca, *Global Navigation Satellite System* (GNSS), entre outros.

Em relação aos sensores, importa referir que estes podem ser categorizados em físicos ou químicos.

Enquanto os sensores físicos medem quantidades físicas como temperatura ou humidade, os sensores químicos transformam informações químicas (p. ex. concentração de determinada substância) em sinais elétricos. A sua utilização deverá ter em consideração algumas características, tais como sensibilidade, compatibilidade com o meio em que vão ser instalados, frequência de operação e robustez (Choudhary e Jain, 2016).

2.2.3.2 Tecnologias da camada de rede

A camada de rede é constituída por grupos de tecnologias e protocolos, divididos por diferentes responsabilidades (Hassan, 2018, Salman e Jain, 2019):

- **Identificação:** Identificadores únicos adstritos a cada dispositivo ou nó que se conecta à rede, de forma a que sejam facilmente localizados e identificados. Exemplos: *Uniform Resource Identifier* (URI); *Electronic Product Code* (EPC).
- **Comunicação:** Meios de comunicação com/sem fios utilizados para que os nós existentes na rede possam comunicar entre si ou com a camada de *middleware*. Exemplos: *Near-Field Communication* (NFC); *Ultra-Wide Bandwidth* (UWB); *Wi-Fi*; 5G; *Bluetooth Low Energy* (BLE); *Long-Range Wide-Area Network* (LoRaWAN).
- **Segurança:** Mecanismos adicionais para incrementar a segurança das comunicações que ocorrem na camada de rede. Exemplos: *Internet Protocol Security* (IPsec); *Transport Layer Security* (TLS).

A seleção das tecnologias de comunicação está dependente do cenário de implementação e respetivos requisitos. A Tabela 2.3 apresenta um sumário comparativo entre diferentes aplicações possíveis e o conjunto de tecnologias mais adequado.

Requisito	**Cenário**	**Caso de uso**	**Tecnologias**
Tipo de utilizador	Humano	*Smartphone*	LTE/LTE-A, 5G, Wi-Fi, UWB
	Máquina	Sensores de monitorização	Blueetooth/BLE, ZigBee, LPWAN, Wi-Fi, UWB
Taxa de dados	Elevada	*Streaming* de vídeo	LTE/LTE-A, 5G, UWB, Wi-Fi
	Reduzida	Medição de corrente elétrica	NB-IoT, Sigfox, LoRa, ZigBee
Latência	Sensível a atrasos	Veículos autónomos	LTE/LTE-A, 5G, Wi-Fi/Wi-Fi, LTE-M
	Tolerante a atrasos	Sensores de gestão de resíduos	ZigBee, Sigfox, NB-IoT, LoRa
Cobertura	Longo alcance	Sensores em campos agrícolas	LTE/LTE-A, 5G, LoRa, Sigfox, NB-IoT, LTE-M
	Alcance reduzido	Eletrodomésticos inteligentes	Bluetooth/BLE, ZigBee, Wi-Fi
Energia	Baixo consumo	Rastreio de posicionamento	Bluetooth, ZigBee, LTE/LTE-A, 5G, Wi-Fi
	Muito baixo consumo	Monitorização de níveis de poluição	BLE, Wi-Fi, LPWAN, LoRa, Sigfox, LTE-M, NB-IoT
Confiabilidade	Crítica	Monitorização de doentes em tempo-real	LTE/LTE-A, 5G, Wi-Fi/Wi-Fi
	Não-crítica	Sensores em campos agrícolas	LPWAN, LoRa, Sigfox, LTE-M, NB-IoT
Mobilidade	Elevada	Veículos autónomos	LTE/LTE-A, 5G
	Baixa	Semáforos inteligentes	LPWAN, ZigBee, Bluetooth/BLE

Tabela 2.3: Comparativo de tecnologias de comunicação com aplicabilidade na IoT (adaptado de Ding et al., 2020 e Oppermann et al., 2005)

2.2.3.3 Tecnologias da camada de *middleware*

A camada de *middleware* é composta pelas seguintes tecnologias (Al-Fuqaha et al., 2015, Hassan, 2018):

- ***Service Discovery*:** Protocolos utilizados em ambientes escaláveis e heterogéneos para o registo e descoberta de serviços a serem utilizados por aplicações e utilizadores. Exemplos: *Universal Plug and Play* (UPnP); *Multicast DNS* (mDNS); *DNS Service Discovery* (DNS-SD).

- **Troca de dados:** Protocolos necessários à gestão de um grande volume de dados derivado do número de nós conectados numa infraestrutura IoT. Exemplos: *Extensible Messaging and Presence Protocol* (XMPP); *Message Queue Telemetry Transport* (MQTT).

- **Computação:** Unidades de processamento de grandes quantidades de dados e gestão de sensores. Exemplos: utilização de *hardware* como um Arduino; serviços *cloud*.

2.2.3.4 Tecnologias da camada aplicacional

De acordo com Gigli e Koo, 2011, a camada aplicacional é formada pelo seguinte conjunto de tecnologias:

- **Serviços de identidade:** Exigem a existência de um identificador adstrito a cada nó ou dispositivo presente na rede, sendo relevantes na medida em que fomentam o controlo desses itens em larga escala. Exemplo: aplicação de rastreio de mercadorias dentro de um armazém.

- **Serviços de agregação de informação:** Resumem os dados sensoriais em bruto oriundos de diversos dispositivos. Exemplo: sistema de controlo e monitorização para uso na produção agrícola.

- **Serviços colaborativos:** Resultam da combinação de serviços de agregação de informações e são utilizados para apoio na tomada de decisões. Exemplo: uma casa inteligente que contém um sistema de segurança e termostatos inteligentes que promovem no seu conjunto a segurança e eficiência energética tendo por base os dados de ambos.

- **Serviços ubíquos:** Com o objetivo de tornarem serviços colaborativos acessíveis a qualquer momento e a partir de qualquer lugar. Exemplo: acesso e controlo de uma casa inteligente através de um computador ou dispositivo móvel com ligação à Internet.

2.2.3.5 Tecnologias da camada de negócio

A camada de negócio pode ser dividida em 2 grupos de tecnologias (Al-Fuqaha et al., 2015):

- **Semântica:** Extração de conhecimento a partir do ambiente IoT. Exemplos: *Sensor Model Language* (SensorML); *Media Types for Sensor Markup Language* (SenML).
- **Análise de *big data*:** Análise em tempo-real de grandes quantidades de dados gerados pelo ambiente IoT. Exemplos: *Apache Spark*; *Apache Kafka*.

2.2.4 Dispositivos IoT

A Figura 2.3 ilustra os diferentes aspetos que podem caracterizar os dispositivos IoT, encontrando-se divididos pelas categorias:

- **Criticidade:** Indica o nível de criticidade do dispositivo em relação ao seu impacto global no processo e quão fácil é de reparar ou substituir.
- **Função:** Descreve a função ou conjunto de funções do dispositivo.
- **Gestão de interface:** Assinala como o dispositivo pode ser configurado, desligado/ligado ou suscetível de outra forma de controlo.
- **Relações:** Enumera as diferentes relações existentes entre o dispositivo e o ambiente, sistemas ou outros dispositivos e processos.

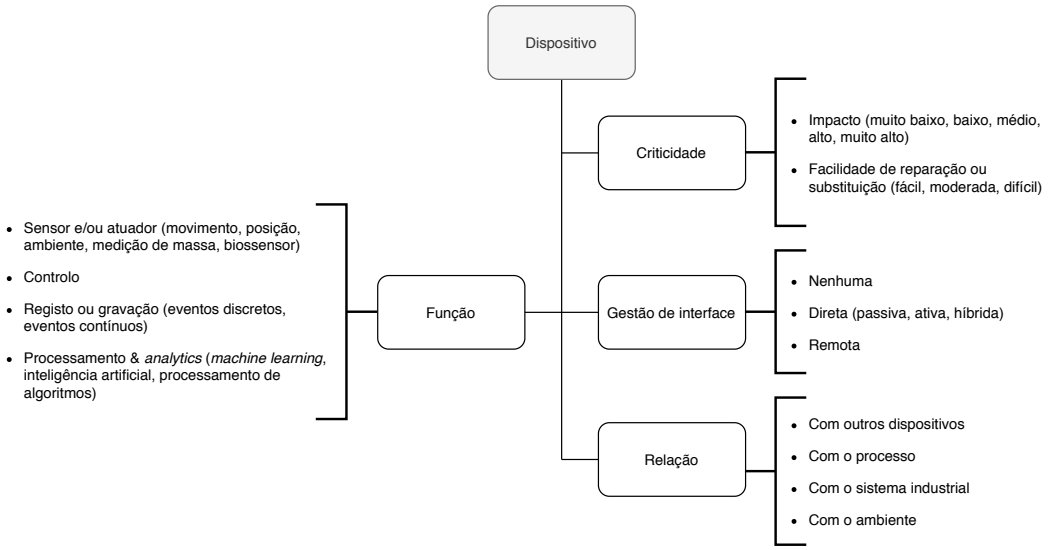


Figura 2.3: Caraterísticas de dispositivos IoT (adaptado de Boyes et al., 2018)

Os dispositivos IoT podem ser compostos por múltiplos sensores e/ou atuadores, de modo a incluírem uma ou mais funções. Em relação aos sensores, estes podem

ser definidos através das categorias (de Morais et al., 2019, Almazaydeh et al., 2016, Safeopedia, 2019a):

- **Acústico:** Ativados através de ondas sonoras, registando alterações acústicas (p. ex. sensores piezoelétricos ou microfones).
- **Ambiente:** Recolhem dados relacionados com o ambiente ou espaço em redor (p. ex. sensores de temperatura, luminosidade, pressão atmosférica e humidade).
- **Biosensor:** Recolhem sinais vitais e/ou informações biológicas de seres humanos ou animais (p. ex. sensores para monitorizar a quantidade de batimentos cardíacos).
- **Elétrico:** Aplicados em redes de eletricidade tendo em vista a sua monitorização (p. ex. sensores para monitorizar o consumo de energia, tensão e outros aspetos).
- **Força / carga:** Ativados por forças externas, registando a deformação ou intensidade protagonizada por essas forças (p. ex. medidor de velocidade).
- **Hidráulico:** Recolhem propriedades de líquidos (p. ex. sensores para medir os níveis de água e intensidade de fluxo).
- **Identificação:** Representa uma semântica ou identidade no sistema IoT (p. ex. etiquetas RFID e NFC).
- **Interação:** Dispositivos ativados manualmente para acionar um evento (p. ex. através de um botão).
- ***Machine vision:*** Capturam imagens que são processadas por um computador e produzem informação (p. ex. deteção da presença de trabalhadores em zonas restritas).
- **Movimento:** Percecionam o movimento de pessoas ou coisas num determinado contexto (p. ex. através de acelerómetros e giroscópios).
- **Posição:** Possibilitam aferir a posição de um objeto a nível *outdoor* (p. ex. através de GNSS) ou no âmbito *indoor* (p. ex. via BLE *beacons*).
- **Presença:** Detetam a entrada/saída de pessoas, animais ou objetos num determinado espaço (p. ex. através de sensores de infravermelhos).
- **Química:** Detetam a presença de substâncias químicas no ar ou na água (p. ex. sensores de fumo, gás ou pH).

Em relação aos atuadores, apesar de serem raramente visíveis durante as operações, o seu efeito pode ser sentido ao nível de veículos, máquinas industriais e quaisquer outros equipamentos eletrónicos que envolvam algum grau de automação tecnológica.

Podem ser separados em quatro categorias tendo em conta o papel que desempenham num sistema de IoT (AVSystem, 2019):

- **Lineares:** Possibilitam o movimento de objetos ou elementos em linha reta através de movimentos *pull* e *push*.
- **Motores:** Permitem movimentos rotacionais precisos de componentes ou objetos na sua totalidade.
- **Relés:** Controlam a energia de interruptores de lâmpadas, veículos a motor, entre outros.
- **Solenoides:** Utilizados por eletrodomésticos como parte de mecanismos de bloqueio e acionamento, servindo também de controladores em sistemas de monitorização de fugas de gases ou líquidos.

2.3 IoT na segurança industrial

Os avanços tecnológicos verificados no campo da IoT acabaram por promovê-la enquanto elemento relevante no domínio da monitorização do ambiente laboral e da saúde de trabalhadores. É possível instalar dispositivos em várias localizações para monitorizar condições ambientais (p. ex. níveis de humidade), bem como ligar dispositivos ao corpo humano para avaliar condições físicas em tempo-real (p. ex. batimentos cardíacos) (F. Wu et al., 2017, T. Wu et al., 2017).

Esta constante monitorização do ambiente industrial proporcionada pela IoT, permite identificar situações de perigo em tempo útil, bem como auxiliar os trabalhadores a não cometerem erros que coloquem em causa a sua própria segurança ou a de terceiros (EU-OSHA, 2018).

A maioria das aplicações da IoT no campo da segurança surge com o intuito de monitorizar e avaliar riscos, apresentando as seguintes valências globais (Kanan, 2016):

- Alerta em tempo-real de possíveis riscos (p. ex. colisões envolvendo veículos);
- Identificação de possíveis riscos para posterior análise e promoção de um local de trabalho seguro;
- Integração de múltiplos sensores heterogéneos numa única plataforma;
- Existência de um sistema de recolha de dados com baixo consumo de energia.

2.3.1 Soluções académicas

Mayton et al., 2012, propõe um sistema de monitorização constante do ambiente industrial, composto por três componentes principais: dispositivo com sensores, estações e câmeras. Os dispositivos equipados com sensores possuem vários módulos para

deteção de gases perigosos, poeira, ruído, níveis de iluminação e altitude. Esses dados são transmitidos para estações que também têm outros sensores e uma câmera de baixa potência. Nesta unidade, toda a informação oriunda de sensores e câmeras é agrupada e enviada para um servidor através da rede *Global System for Mobile Communications* (GSM) ou Wi-Fi. Mais tarde, os gestores de segurança podem receber os dados e aferir riscos, bem como determinar a localização dos trabalhadores.

Lee et al., 2009, refere a possibilidade de criar um sistema móvel para monitorizar eventuais riscos de queda que os trabalhadores possam sofrer. São utilizadas unidades móveis de deteção que são colocadas em locais onde podem ocorrer quedas, sendo compostas por sensores híbridos (infravermelhos e ultrassons), alarmes sonoros, baterias para fornecimento de energia e transmissores de radiofrequência. A utilização de sensores híbridos justifica-se pela necessidade de distinção entre a queda de um objeto e a de um ser humano através da temperatura do corpo em movimento. Além disso, quando um trabalhador se aproxima de uma zona de perigo, os alarmes são acionados.

Chae e Yoshida, 2010, sugere um sistema de segurança através da utilização da tecnologia RFID, tendo o foco primário na garantia de anti-colisão de trabalhadores e equipamentos industriais. Os trabalhadores possuem etiquetas RFID, enquanto as máquinas como escavadoras ou qualquer outro equipamento industrial tem, além de etiquetas, leitores de RFID. O principal objetivo é que o leitor detecte a proximidade dos trabalhadores e que estes possam ser alertados de tal cenário.

Num cenário de segurança industrial, o desempenho das baterias utilizadas em sistemas IoT assume uma enorme relevância, de modo a promover a fiabilidade dos sistemas. Contudo, a reposição de baterias poderá revelar-se num custo considerável do ponto de vista operacional. Neste sentido, Thomas et al., 2011, apresenta um sistema que dispensa baterias. Através da tecnologia *Ultra High Frequency* (UHF), foi criado um protótipo com etiquetas semi-passivas que foram colocadas nos capacetes dos trabalhadores. Instalaram-se também dispositivos em maquinaria, com a capacidade de emissão de sinais UHF para as etiquetas passivas, de modo a que isso despoletasse um sinal sonoro no capacete e o trabalhador fosse assim alertado para o facto de estar numa zona de perigo. Esta zona é automaticamente definida através da força de sinal necessária para ativar as etiquetas previamente instaladas em cada um dos capacetes, tendo sido possível enviar alertas a uma distância máxima de 16,5 metros.

2.3.2 Soluções comerciais

Esta subsecção apresenta algumas soluções comerciais existentes no mercado que combinam múltiplos sensores com o intuito de criar dispositivos IoT que possam ser aplicados na indústria no âmbito da promoção da segurança e saúde no trabalho.

Figura 2.4: Dispositivo GH5200 (Teltonika, 2020)

2.3.2.1 GH5200

O GH5200 (ver Figura 2.4) é um dispositivo configurável de uso individual com conetividade GNSS, GSM e BLE.

Destina-se a trabalhadores que desempenham atividades independentes, ou não, da supervisão de terceiros (p. ex. funcionários que trabalham fora do período normal de trabalho). Através da combinação de tecnologias de comunicação com sensores como acelerómetro e giroscópio, é possível utilizar o dispositivo em alguns cenários, tais como (Teltonika, 2020):

- Deteção de excesso de velocidade, quedas ou ausência de movimento;
- Alarmes manuais despoletados pelos utilizadores;
- Configuração de cercas geográficas de segurança;
- Comunicação de voz bidirecional;
- Monitorização de posição em tempo-real.

2.3.2.2 RASOR

O RASOR (ver Figura 2.5) é um dispositivo que recolhe e integra dados em tempo-real com o objetivo de proporcionar uma maior segurança aos trabalhadores durante o desempenho das suas funções laborais, através da monitorização da presença de perigos como ruído, gases, poeiras, entre outros.

Permite agregar dados de outros dispositivos através da tecnologia BLE, tem conetividade GNSS para a registo da localização dos operadores e GSM, de forma a enviar os dados para uma plataforma *web* que centraliza toda a informação em tempo-real. Também está equipado com um botão para sinalizar situações de "pânico" e com um mecanismo de deteção de quedas (Reactec, 2020).

Figura 2.5: Dispositivo RASOR (Reactec, 2020)

Figura 2.6: Capacete HC1 (Guardhat, 2020)

2.3.2.3 HC1

O HC1 (ver Figura 2.6) é um capacete que oferece uma monitorização em tempo-real do contexto em que se insere através de sensores de temperatura, humidade, pressão, nível de ruído e proximidade. Deteta a ocorrência de quedas e fornece compatibilidade com várias tecnologias de comunicação como UWB, Zigbee, Wi-Fi, LTE, NFC e BLE.

Pode funcionar em modo *offline* e o posicionamento em tempo-real do dispositivo pode ser obtido quer a nível *indoor* através da existência de uma infraestrutura de *beacons*, quer a nível *outdoor* através de GNSS.

2.3.3 Desafios

De acordo com a EU-OSHA, 2018, a utilização da tecnologia com o objetivo de incrementar a segurança a nível industrial está naturalmente relacionada com desafios

que devem ser tidos em consideração aquando da sua implementação.

Um dos desafios passa pelo desenvolvimento de sistemas IoT que apresentem grande fiabilidade, para que não forneçam informações que conduzam a decisões erradas.

O aumento da utilização de *wearables*, IoT, entre outras tecnologias, e o grande volume de dados daí derivado, traduzir-se-á na necessidade de adquirir recursos humanos especializados que possam auxiliar as organizações na gestão da informação e complexidade inerente a tais tecnologias.

De outro modo, a memória corporativa poderá ser afetada negativamente. Apesar da IoT ter a capacidade de fomentar o acesso a formações ou procedimentos de trabalho a qualquer momento, tal facto poderá criar uma dependência excessiva de dispositivos eletrónicos, numa ótica em que será mais difícil encontrar a informação procurada do que propriamente memorizá-la. Esse cenário poderá representar um problema se, por alguma razão, não for possível aceder à informação pretendida, estiver corrompida ou desatualizada.

Dependendo da indústria e do contexto em que o sistema IoT é utilizado, pode ser importante ter em atenção o cumprimento de padrões ou diretivas, garantir a eficiência energética dos dispositivos utilizados, conetividade e latência, a par da segurança global do sistema e privacidade da informação nele existente (Thibaud et al., 2018).

Capítulo 3

Metodologia

Este capítulo aborda a metodologia *Design Science Research* que foi utilizada na realização deste trabalho, relacionando-a com a estratégia de investigação adotada.

3.1 *Design Science Research*

A metodologia *Design Science Research* foi selecionada para a realização deste trabalho por tratar-se de uma metodologia utilizada frequentemente em sistemas de informação, nomeadamente ao nível da produção de conhecimento, tendo em vista o desenvolvimento de modelos, *frameworks*, arquiteturas, princípios de *design*, métodos, entre outros (Hevner et al., 2004, Manson, 2006).

Trata-se de uma metodologia que procura encontrar melhorias ou novas soluções para múltiplos problemas, quer sejam novos ou não, através da obtenção de conhecimento teórico ou prático. O principal objetivo é que esse conhecimento se traduza na resolução de problemas reais com relevância para as organizações (Gregor e Hevner, 2013).

Apesar da literatura existente ter várias propostas para a representação e implementação da metodologia, os diferentes modelos possuem em comum as fases: identificação do problema para o qual a solução deve ser encontrada; desenho e criação do artefacto que representa a solução para o problema; e a avaliação do artefacto (Haj-Bolouri, 2015, Gerber et al., 2015). A Figura 3.1 ilustra uma proposta de definição da metodologia através de 5 elementos.

O processo de pesquisa inicia-se com a consciencialização de um determinado problema. Essa tomada de consciência pode ter múltiplas origens, tais como experiências, desenvolvimento de novas tecnologias, revisão de literatura existente, entre outras.

Durante a fase de sugestão, procuram-se potenciais elementos que façam parte do

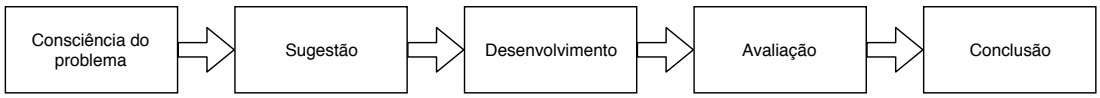


Figura 3.1: Elementos da metodologia *Design Science Research* (adaptado de Manson, 2006)

artefacto a ser desenvolvido e avaliado. Trata-se de uma etapa em que vários pesquisadores poderão obter resultados distintos para o mesmo problema em estudo.

Após as etapas de tomada de consciência do problema e sugestão, existe a necessidade de proceder ao desenvolvimento de um ou mais artefactos que possam ser uma proposta de solução. As técnicas de desenvolvimento dependem do tipo de artefacto que se pretende obter.

A avaliação do artefacto que resulta da aplicação da metodologia é crucial para fundamentar a sua importância e validade. Hevner et al., 2004, sugere que a avaliação pode ocorrer através de 5 formas:

- **Observacional:** Estudo pormenorizado do artefacto num contexto de ambiente empresarial.
- **Analítica:** Análise da estrutura do artefacto no que diz respeito a qualidades estáticas; estudo da forma como este se incorpora na arquitetura técnica; demonstração dos seus atributos ideais; estudo das suas qualidades dinâmicas.
- **Experimental:** Estudo num ambiente controlado para determinar as qualidades do artefacto; execução com dados fictícios num ambiente de testes.
- **Testes:** Implementação de interfaces para determinar eventuais falhas ou identificar defeitos; execução de testes de cobertura de métricas para implementação do artefacto.
- **Descritiva:** Utilização de bases de dados de conhecimento para fundamentar argumentos acerca da qualidade do artefacto; construção de cenários detalhados para demonstrar a sua utilidade.

Adicionalmente, alguns autores sugerem a utilização de *focus groups* num contexto de desenvolvimento e avaliação do artefacto. A condução de avaliações intermédias poderá ser vista como uma forma de melhoria contínua até que a avaliação final do artefacto aconteça (Haj-Bolouri, 2015).

3.2 Estratégia de investigação

A estratégia de investigação utilizada na presente dissertação pressupõe a aplicação da metodologia *Design Science Research*. Tendo em consideração as várias propostas de modelo existentes na literatura, optou-se por selecionar a de Manson, 2006, por

considerar-se a sua aplicabilidade no presente trabalho de investigação. De acordo com esse modelo, a estratégia caracteriza-se pelas seguintes atividades:

1. **Consciência do problema:** Revisão de literatura acerca da relevância e evolução da saúde e segurança dos trabalhadores em âmbito industrial, a par dos conceitos que explicam a IoT.

2. **Sugestão:** Levantamento das várias tecnologias IoT e respetiva relação com a temática da segurança industrial, de forma a mitigar riscos adstritos à atividade laboral em contexto industrial.

3. **Desenvolvimento:** Elaboração de uma *framework* que possa ser adotada pelos vários setores da indústria com o objetivo auxiliar a seleção de tecnologias IoT que permitam incrementar a segurança dos trabalhadores.

4. **Avaliação:** Avaliação da *framework* através da realização de entrevistas a especialistas da área de saúde e segurança no trabalho e de IoT. Nesta fase, pretende-se avaliar a utilidade, concordância e recolher sugestões de melhoria.

5. **Conclusão:** Reflexão acerca dos resultados obtidos na fase de avaliação. Poderão introduzir-se alterações à versão inicial da *framework*, no seguimento das críticas e sugestões resultantes das entrevistas realizadas.

Capítulo 4

Framework para seleção de tecnologias IoT

Este capítulo apresenta uma *framework* para auxiliar a seleção de tecnologias IoT para incrementar a segurança industrial. Deste modo, são referenciados os pressupostos que serviram de base à elaboração do artefacto, procedendo-se posteriormente à sua avaliação e discussão.

4.1 Pressupostos

Tendo por base a revisão de literatura com foco na segurança industrial, IoT e relação entre ambas as áreas, é possível afirmar que:

- Os trabalhadores industriais encontram-se expostos a múltiplos perigos adstritos à atividade laboral e que podem afetar negativamente a sua saúde e segurança (ILO, 2019). É por isso fundamental adotar mecanismos que promovam o seu bem-estar físico e mental, bem como reduzir quaisquer riscos que possam estar presentes em contexto laboral (DIMULESCU e DOBROTĂ, 2018).
- A definição de quais os perigos e riscos que afetam os trabalhadores depende da atividade económica e setor industrial em causa. Existem setores que são caraterizados naturalmente por um maior número de perigos devido a especificidades da própria indústria, nomeadamente processos, tipologia de máquinas e equipamentos envolvidos, localização das operações, entre outras (IPIECA/OGP, 2006, Gardner, 2003, FESETE, 2010, Niven e McLeod, 2009).
- A prevenção de perigos pode iniciar-se com a enumeração das atividades e procedimentos que possam representar riscos para os trabalhadores; instalação de sistemas de controlo de processos; desenvolvimento de sistemas de monitorização para despoletar alarmes atempadamente; adoção de sistemas de controlo,

como o corte de energia elétrica; e mecanismos físicos de proteção, como válvulas (Vadimovna e Sergeevich, 2017).

- O conjunto de medidas que devem ser adotadas como resposta aos perigos existentes na indústria, pode ser determinada com recurso a uma hierarquia composta por vários níveis, tais como: eliminação física do perigo; substituição de substâncias por outras que apresentem menor risco; isolamento dos trabalhadores através de controlos de engenharia, como modificações introduzidas em maquinaria; aplicação de controlos administrativos, como a alteração do modo como as tarefas são executadas; e, por último, a utilização de equipamentos de proteção individual (CDC, 2015).

- A monitorização regular de ambientes industriais favorece a identificação de potenciais cenários de perigo em tempo útil e reduz drasticamente os riscos a si adstritos (EU-OSHA, 2018).

- A IoT carateriza-se por um conjunto de objetos físicos com tecnologia incorporada, que comunicam e interagem entre os seus estados internos e o ambiente exterior (Gartner, 2019). São objetos descentralizados com ligação à Internet (Minerva et al., 2015), que apresentam caraterísticas como a interoperabilidade; orientação a serviços; modularidade e flexibilidade; comunicação multi-ponto; dinamismo e possibilidade de configuração em *runtime*; e facilidade de instalação (Wang et al., 2017).

- Um sistema IoT pode ser composto por múltiplas camadas definidas naturalmente pela complexidade exigida em cada cenário (Al-Fuqaha et al., 2015). A camada de perceção é comum às diversas arquiteturas, sendo formada por sensores que percecionam o ambiente externo, como um sensor de gás, e atuadores que realizam ações, como o controlo um interruptor. Igualmente comum, a camada de rede é constituída por mecanismos e protocolos que transportam dados de/para a camada de perceção (Khan et al., 2012).

- A utilização de tecnologias IoT pode ser relevante no campo da monitorização de ambientes industriais e consequente promoção da saúde e segurança dos trabalhadores. Esta monitorização pode acontecer ao nível do ambiente laboral, como a medição da temperatura ambiente (F. Wu et al., 2017), e ocorrer ao nível individual de cada trabalhador através, por exemplo, da avaliação em tempo-real das suas condições físicas (T. Wu et al., 2017).

4.2 Proposta

Os pressupostos referidos na secção anterior conduziram à elaboração de uma proposta de *framework* para auxiliar a seleção de tecnologias IoT.

A *framework* tem por objetivo favorecer o levantamento de todos os controlos necessários para a mitigação de riscos que possam afetar negativamente a saúde e segurança dos trabalhadores de diferentes setores da indústria, identificar eventuais requisitos ou restrições que devam ser considerados, conduzindo à seleção de tecnologias que devem fazer parte do sistema IoT.

A Figura 4.1 representa os principais componentes do artefacto desenvolvido.

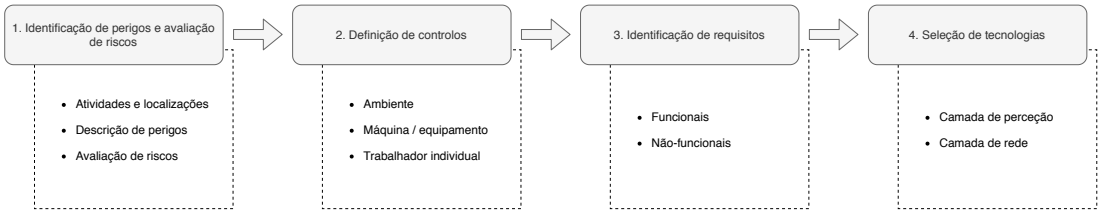


Figura 4.1: *Framework* para seleção de tecnologias IoT no âmbito da segurança industrial

4.2.1 Identificação de perigos e avaliação de riscos

O primeiro passo da *framework* é o levantamento de todos os perigos existentes em contexto laboral que podem colocar em causa a segurança e saúde dos trabalhadores. Estes perigos variam de acordo com a indústria e especificidades de cada entidade empresarial.

A Figura 4.2 apresenta um fluxograma para auxiliar a identificação e avaliação dos perigos afetos a cada departamento das organizações, antecedendo a fase de definição de controlos.

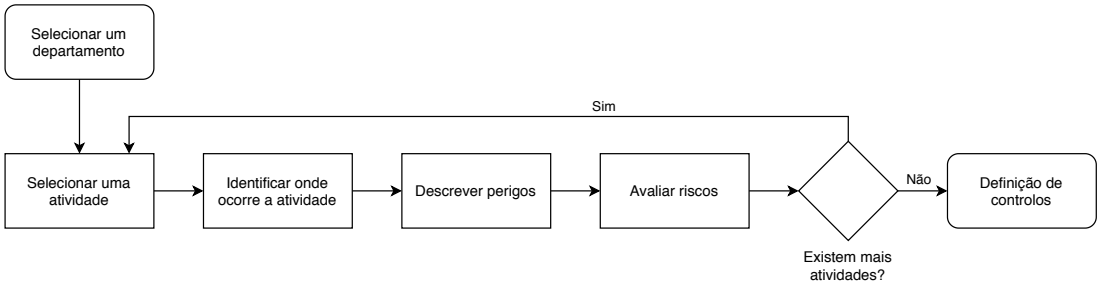


Figura 4.2: Fluxograma para a identificação de perigos e avaliação de riscos por departamento

A listagem dos perigos adstritos a cada atividade pode ser obtida através de (Ramesh et al., 2017):

- Inspeção do local onde a atividade ocorre;
- Revisão de incidentes passados;
- Leitura de normas legais específicas da atividade;

- Verificação exaustiva de todas as tarefas e sub-tarefas;
- Inquéritos junto dos trabalhadores acerca dos perigos que eles identificam.

A descrição dos perigos deve considerar a sua tipologia, causas e consequências, ajudando a identificar eventuais relações que possam existir entre perigos semelhantes (p. ex. presença de gases e poeiras). A Tabela 4.1 apresenta as diferentes naturezas do perigo – geográfico, físico, químico, biológico, ergonómico e psicossocial –, bem como exemplos de causas e consequências.

Tipo	**Causa**	**Consequência**
Geográfico	Problemas de comunicação	Perda de contato
Físico	Iluminação insuficiente	Quedas
Químico	Poeiras	Problemas respiratórios
Biológico	Higiene deficiente	Infeções
Ergonómico	Postura incorreta	Fadiga
Psicossocial	Isolamento	Ansiedade

Tabela 4.1: Exemplos de perigos de várias tipologias (IPIECA/OGP, 2006, Gardner, 2003, FESETE, 2010, Niven e McLeod, 2009)

Em relação à avaliação de riscos, esta deve considerar a sua probabilidade de ocorrência e severidade, de forma a aferir, por exemplo, a prioridade com que devem ser implementados os controlos.

A Figura 4.3 demonstra uma matriz de análise qualitativa que pode ser utilizada para rotular os riscos existentes em baixo (B), moderado (M), alto (A) ou extremo (E).

Assim, espera-se que a aplicação da primeira etapa da *framework* produza um artefacto semelhante à Tabela 4.2, servindo de ponto de partida para a definição dos controlos necessários à mitigação dos riscos identificados.

			Perigos			
Departamento	**Atividade**	**Localização**	**Tipo**	**Causa**	**Consequência**	**Risco**
Operações	Armazenamento de matéria-prima	Armazém A.1	Químico	Poeira	Problemas respiratórios	M
		Armazém A.2				

Tabela 4.2: Exemplo da identificação de perigos e avaliação de riscos

4.2.2 Definição de controlos

Nesta fase importa definir quais os controlos e onde estes devem ser aplicados de forma a mitigar os riscos identificados anteriormente. A Figura 4.4 demonstra o fluxograma associado a esta fase.

A aplicação de controlos pode ser dividida em três categorias:

Severidade / Probabiidade	**Insignificante** (p. ex. não requer qualquer tratamento)	**Reduzida** (p. ex. requer primeiros socorros)	**Moderada** (p. ex. requer tratamento médico)	**Considerável** (p. ex. grave e requer tratamento hospitalar)	**Catastrófica** (p. ex. morte ou incapacidade permanente)
Raro (< 3%)	Baixo	Baixo	Baixo	Moderado	Moderado
Improvável (3% a 10%)	Baixo	Moderado	Moderado	Alto	Alto
Moderado (10% a 50%)	Moderado	Moderado	Alto	Extremo	Extremo
Provável (50% a 90%)	Moderado	Alto	Extremo	Extremo	Extremo
Muito provável (> 90 %)	Moderado	Alto	Extremo	Extremo	Extremo

Figura 4.3: Matriz qualitativa de avaliação de riscos (adaptado de Collins et al., 2014)

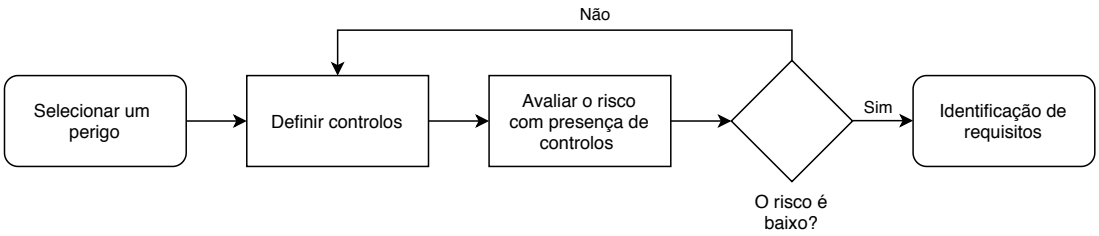


Figura 4.4: Fluxograma para a definição de controlos

- **Ambiente:** Controlos aplicados em determinadas localizações de instalações fabris, quer seja a nível *indoor* ou *outdoor*.
- **Máquinas / Equipamentos:** Controlos destinados a máquinas ou equipamentos.
- **Trabalhador individual:** Controlos atribuídos individualmente a cada um dos trabalhadores que podem ficar expostos ao perigo.

Estes controlos são relevantes numa ótica de mitigação de perigos e riscos, podendo ser vistos como medidas proactivas (p. ex. instalação de um sistema de corte de energia elétrica numa máquina para que a impeça de operar em determinadas condições) ou reativas (p. ex. através da atribuição de um dispositivo de deteção de quedas a cada trabalhador).

A definição de controlos poderá incidir em um ou vários âmbitos em simultâneo, dependendo do grau de robustez e tolerância a falhas que se pretende alcançar. Por exemplo, no caso da implementação de um sistema para prevenção de colisões entre

veículos e pessoas, apesar deste ser possível mediante a inclusão de um sistema de deteção de obstáculos e ativação dos travões do veículo em questão, poderá fazer sentido atribuir dispositivos IoT com a capacidade de deteção de colisões aos trabalhadores expostos a esse perigo. Assim, não só os veículos teriam a capacidade de evitar uma colisão, como os trabalhadores poderiam agir em tempo útil.

Neste contexto, importa destacar a importância de incrementar o número de controlos de acordo com a severidade e probabilidade de cada risco. Riscos críticos devem apresentar naturalmente um maior número de controlos comparativamente com riscos mais baixos, de modo a reduzir ao máximo a sua severidade e probabilidade de ocorrência.

A Tabela 4.3 apresenta exemplos de controlos que podem ser implementados através da utilização de tecnologias IoT, tendo em vista a minimização do risco.

Âmbito da aplicação	**Exemplos**
Ambiente	- Monitorização de níveis de ruído; - Controlos de temperatura; - Controlos de níveis de gases ou poeiras.
Máquinas / Equipamentos	- Sistemas de anti-colisão; - Sistemas de corte de energia; - Deteção de excesso de velocidade.
Trabalhador individual	- Monitorização de posicionamento; - Monitorização de frequência cardíaca; - Deteção de ausência de movimento.

Tabela 4.3: Exemplos de controlos que podem ser suportados por tecnologias IoT

A última etapa do processo de definição de controlos carateriza-se pela execução de uma nova avaliação de riscos, permitindo um comparativo entre o risco esperado antes e após a aplicação de controlos. Enquanto a severidade e probabilidade de ocorrência não for baixa, deve-se considerar a implementação de mais controlos.

A implementação desta etapa da *framework* deverá conduzir à elaboração de um artefacto semelhante à Tabela 4.4, para que seja possível enumerar os controlos a aplicar e aferir posteriormente os requisitos funcionais e não-funcionais.

4.2.3 Identificação de requisitos

A Figura 4.5 apresenta a fase posterior à definição de controlos, que corresponde ao levantamento de requisitos e restrições que podem condicionar a seleção de tecnologias da camada de perceção e de rede que fazem parte da solução de IoT.

Os requisitos funcionais procuram descrever a solução no seu âmbito funcional, ao nível do comportamento e ações que devem existir; enquanto que os não-funcionais

Perigos				Controlos			
Tipo	**Causa**	**Consequência**	**Risco**	**Âmbito**		**Descrição**	**Risco**
Químico	Poeira	Problemas respiratórios	M	Ambiente	Armazém 1 Armazém 2	Monitorização de níveis de poeira na área de trabalho	B
				Equipamento	Silo 1 Silo 2 Silo 3	Sistema de alarme sonoro e visual instalado junto aos equipamentos	
				Trabalhador	Departamento de operações	Dispositivo de leitura de níveis de poeira com alarme vibratório	

Tabela 4.4: Exemplo da definição de controlos

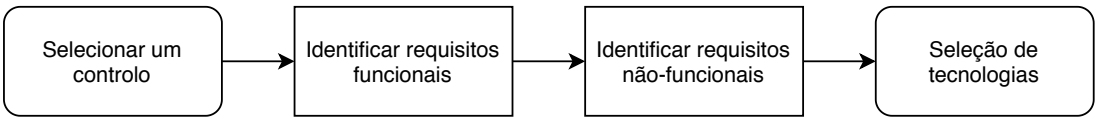


Figura 4.5: Fluxograma para avaliação de requisitos

descrevem propriedades ou restrições que devem ser tidas em consideração na elaboração da solução final (Sommerville e Sawyer, 2003).

Determinados meios industriais podem condicionar a seleção de tecnologias. Por exemplo, a exploração mineira, uma vez que a tecnologia de posicionamento GNSS não é indicada para ambientes *indoor*.

A resposta de emergência é outro aspeto a considerar, uma vez que a aplicação do controlo poderá ter que despoletar alarmes automáticos cruciais para a robustez do sistema IoT, enquanto solução de promoção de segurança para os trabalhadores. Por exemplo, num cenário em que um trabalhador sofre uma queda, não só é relevante detetar a ocorrência desse evento como notificar imediatamente terceiros (p. ex. abertura automática de um canal de voz com uma central de emergência e o trabalhador).

A Tabela 4.5 apresenta alguns requisitos e restrições que poderão estar associados aos controlos que se pretendem aplicar.

4.2.4 Selecção de tecnologias

Tendo em consideração quais são controlos e onde estes devem ser aplicados, a par das restrições existentes, procede-se à definição das tecnologias que materializam os requisitos.

Neste campo são equacionadas tecnologias da camada de perceção, como sensores e atuadores, e tecnologias de comunicação que visam a transmissão dos dados provenientes da primeira camada.

De seguida, apresentam-se recomendações para a camada de perceção do sistema IoT de acordo com alguns exemplos de requisitos comuns (de Morais et al., 2019, Almazaydeh et al., 2016, Safeopedia, 2019a):

Tipo	**Exemplos de requisitos**
Funcional	- Alarmes visuais ou sonoros; - Comunicação por voz; - Deteção de quedas; - Deteção de substâncias químicas; - Deteção da presença de equipamentos ou pessoas; - Despoletar alarmes manuais de emergência; - Monitorização de posicionamento; - Monitorização de movimento; - Monitorização de sinais vitais; - Medição de forças e/ou velocidades; - Monitorização de alterações acústicas; - Monitorização de sinais vitais; - Monitorização de temperatura, luminosidade, pressão atmosférica ou humidade; - Prevenção de colisões; - Prevenção de eletrocussão.
Não-funcional	- Ambiente *indoor* ou *outdoor*; - Cobertura elevada, média ou reduzida; - Mobilidade elevada ou reduzida/inexistente; - Identificação do dispositivo IoT.

Tabela 4.5: Exemplos de requisitos funcionais e não-funcionais

- **Alarmes visuais ou sonoros:** Relés para controlar o estado dos alarmes.

- **Deteção de quedas:** Acelerómetros e giroscópios no caso de dispositivos individuais destinados a trabalhadores; Câmeras para alimentarem algoritmos de deteção de quedas.

- **Deteção de substâncias químicas e gases:** Sensores químicos específicos para cada substância. Os mais comuns são sensores de dióxido de carbono, monóxido de carbono, hidrogénio, óxido de nitrogénio, oxigénio, ozono, poluição do ar. A deteção de fumo originado por focos de chamas pode ser possível através de sensores óticos (fotoelétrico) ou por ionização. A existência de espaços confinados configura numa necessidade de deteção do gás sulfureto de hidrogénio (H_2S), sendo este usualmente considerado por equipamentos destinados à medição dos níveis de presença de múltiplos gases.

- **Deteção de presença de equipamentos ou pessoas:** Além das tecnologias de monitorização de posicionamento, podem ser utilizadas etiquetas RFID e NFC, câmeras térmicas.

- **Despoletar alarmes manuais de emergência:** Instalação de uma interface no dispositivo IoT que permita aos trabalhadores pressionarem botões para gerarem determinados tipos de alarmes ou funcionalidade (p. ex. abertura de um canal de voz com terceiros).
- **Monitorização de posicionamento:** A nível *indoor* podem ser utilizadas tecnologias como UWB, Wi-Fi, Bluetooth, etiquetas RFID; enquanto que a nível *outdoor*, as tecnologias mais indicadas são GNSS e UWB.
- **Monitorização de sinais vitais:** Sensores para medição de frequência cardíaca e respiratória.
- **Monitorização de níveis acústicos:** Microfones e sensores piezoelétricos.
- **Identificação de dispositivos IoT**: RFID, NFC, QR codes e códigos de barras.
- **Prevenção de colisões:** RFID, sensores de infravermelhos e câmeras. Alternativamente podem ser utilizadas as tecnologias de monitorização de posicionamento para aferir distâncias e trajetórias.
- **Prevenção de eletrocussão:** Sensores elétricos para verificar a presença de energia elétrica e relés para controlar a passagem de corrente.

A Tabela 4.6 apresenta as recomendações de tecnologias de comunicação para a camada de rede (Ding et al., 2020, Oppermann et al., 2005).

Requisitos		**Recomendações**
Ambiente	*Indoor*	Wi-Fi, Bluetooth, UWB
	Outdoor	LTE, 5G, UWB
Cobertura	Elevada	LTE/LTE-A, 5G, LoRa, NB-IoT, LTE-M
	Reduzida	Bluetooth/BLE, Wi-Fi, UWB
Mobilidade	Elevada	LTE/LTE-A, 5G
	Reduzida	LPWAN, Bluetooth/BLE
Comunicação por voz		LTE, 5G

Tabela 4.6: Tecnologias recomendadas para a camada de rede

4.3 Avaliação

A avaliação da *framework* proposta para auxiliar o processo de seleção de tecnologias IoT com o objetivo de incrementar a segurança dos trabalhadores em contexto industrial, foi realizada através de entrevistas a especialistas na área de IoT e segurança e saúde no trabalho.

Uma vez que o artefacto resultou de um conjunto de pressupostos obtidos por intermédio da revisão de literatura, a realização destas entrevistas procurou aferir a utilidade e validade da *framework* para a realidade industrial, bem como obter eventuais melhorias que pudessem ser incluídas.

Neste contexto, elaborou-se uma apresentação com os objetivos da presente investigação e a *framework* (Apêndice A), para posterior análise de um grupo constituído por dois especialistas em IoT e dois especialistas em segurança e saúde no trabalho (Apêndice B).

Após a apresentação da proposta, foram realizadas três questões:

1. Considera que a *framework* apresentada é útil?
2. Concorda com a *framework*?
3. Quais são as melhorias que propõe?

As questões permitiram aferir a utilidade do artefacto para a área da segurança industrial e suporte à seleção de tecnologias IoT, avaliar a concordância dos especialistas em relação à estrutura apresentada e, por fim, recolher sugestões de alteração ou melhoria que pudessem ser implementadas no decorrer da presente investigação ou incluídas como trabalho futuro.

4.4 Discussão de resultados

Após a avaliação do artefado levada a cabo por especialistas em IoT e segurança e saúde no trabalho, procedeu-se a uma reflexão acerca do *feedback* obtido.

Relativamente à utilidade da *framework*, os inquiridos destacaram a pertinência do artefacto para a promoção da segurança dos trabalhadores em ambientes industriais e a sua aplicabilidade em contexto real. A metodologia proposta para o levantamento de requisitos carateriza-se como outro fator relevante da sua utilidade, uma vez que padroniza esse processo, tornando-o eficaz e promovendo uma poupança de tempo e recursos para as organizações.

Existe uma ampla concordância acerca da versão inicial do artefacto (Apêndice A) que foi apresentada no decorrer das entrevistas. A demonstração da aplicabilidade da *framework* em termos práticos é entendida como uma mais-valia que revela a abrangência de múltiplos aspetos fundamentais a nível industrial (p. ex. diferentes âmbitos da aplicação de controlos para minimização de perigos). Traduz-se, por isso, num modelo que produzirá uma avaliação abrangente das necessidades de segurança e saúde no trabalho, levando consequentemente à seleção de tecnologias IoT.

Não obstante, foram recolhidas algumas sugestões para a melhoria da *framework*, tais como:

- Incluir referência ao gás sulfureto de hidrogénio (H_2S) por ser bastante comum em ambiente industrial, mais concretamente em espaços confinados. Trata-se de um gás tóxico, inflamável e incolor, que é usualmente detetado por equipamentos destinados à medição da presença de múltiplos gases.

- Enfatizar a necessidade de balancear a quantidade de controlos de acordo com a criticidade de cada risco. Riscos com maior probabilidade e impacto, devem possuir um maior número de controlos de forma a minimizar a sua ocorrência e severidade. Em contrapartida, é aceitável que riscos mais baixos apresentem menos controlos.

- Rever as recomendações tecnológicas para a camada de rede do sistema IoT, uma vez que as implementações mais recentes focam-se, por exemplo, em tecnologias como LoRaWAN e 5G, em alternativa a SigFox ou ZigBee.

- Complementar o ponto de seleção de tecnologias, de modo a que estas se possam relacionar melhor com o ambiente industrial em que se inserem. Além da distinção entre *indoor* e *outdoor*, é relevante determinar a existência de materiais que derivado das suas características, sejam fontes de interferências. Neste contexto, destaca-se a presença de paredes de betão que podem simular uma gaiola de Faraday ou a de motores elétricos que criem campos magnéticos.

Após a inclusão da referência ao gás H_2S no ponto 4.2.4 e respetiva associação a espaços confinados, procedeu-se à revisão do ponto 4.2.2 para clarificar a necessidade de adequar o número de controlos à severidade e probabilidade de ocorrência de cada risco. Adicionalmente, no ponto 4.2.4 optou-se por abandonar a recomendação de utilização das tecnologias SigFox e ZigBee para a camada de rede por existirem alternativas mais recentes e robustas.

Entendeu-se que existe a oportunidade de efetuar um estudo mais aprofundado em relação às tecnologias da camada de rede e potenciais interferências que possam existir em ambiente industrial, com o objetivo de colmatar cenários extremos e pontuais. Por exemplo, eventuais restrições temporárias ou permanentes que possam existir para o bom funcionamento de determinada tecnologia numa dada localização. Tais restrições podem configurar na necessidade de recorrer a uma ou várias tecnologias, na tentativa de colmatar o problema. Trata-se, por isso, de um estudo a ser considerado como trabalho futuro, dado que as recomendações atuais da *framework* com base nos requisitos ambiente, cobertura, mobilidade e comunicação por voz, têm utilidade em cenários com condições normais.

Capítulo 5

Conclusão

Este capítulo resume o trabalho desenvolvido no âmbito da presente dissertação, apresenta as principais conclusões e menciona o trabalho que poderá ser realizado futuramente.

No decurso da dissertação foi possível estudar a temática da segurança e saúde no trabalho em contexto industrial, determinar fatores de perigo e as múltiplas medidas que podem ser colocadas em prática para reduzir riscos associados. Procurou-se estudar a IoT nas suas múltiplas dimensões, não apenas ao nível das tecnologias facilitadoras e dispositivos existentes, mas também ao nível da arquitetura para obter uma visão clara acerca das diferentes camadas existentes. Além disso, entendeu-se que seria fundamental estudar a relação da IoT com a segurança industrial, nomeadamente através da identificação de soluções académicas e comerciais.

A revisão de literatura possibilitou o levantamento de um conjunto de pressupostos que conduziram à elaboração de uma *framework* de 4 etapas para ser adotada pelos vários setores da indústria, tendo em vista o apoio na seleção de tecnologias IoT que incrementem a segurança dos trabalhadores a nível industrial.

O artefacto proposto pretende contemplar todos os passos necessários que conduzem à seleção tecnológica, como os procedimentos adstritos à identificação de perigos e avaliação de riscos, a definição de controlos necessários à mitigação dos riscos, e o levantamento de quaisquer requisitos funcionais ou não-funcionais que devam ser considerados.

Optou-se por incluir fluxogramas e diversos exemplos ao longo da explicação detalhada de todos os passos do artefacto, com o objetivo de clarificar todas as etapas e exemplificar o resultado derivado da sua aplicação.

Procedeu-se à avaliação e validação da *framework* através de entrevistas realizadas

a um conjunto de especialistas na área de IoT e segurança e saúde no trabalho, procurando aferir a utilidade da *framework* para a indústria. Por fim, foi possível recolher sugestões de melhoria (p. ex. enfatizar a necessidade de balancear a quantidade de controlos de acordo com a severidade e probabilidade de cada risco) que produziram alterações no documento e considerações para trabalho futuro.

5.1 Limitações

Durante a elaboração do documento ocorreu uma pandemia inesperada à escala mundial, que acabou por condicionar a obtenção de *feedback* em relação ao artefacto apresentado. Apesar de se terem realizado contactos com múltiplos profissionais de segurança e saúde no trabalho de diferentes tipos de indústria, a disponibilidade destes foi manifestamente reduzida devido a condições anormais provocadas pelo evento inesperado. No entanto, foi possível obter *feedback* de profissionais experientes e com percursos profissionais de revelo em multinacionais e indústrias de grande porte.

Outra limitação reside na ausência da aplicação da *framework* num caso de estudo concreto. Apesar do artefacto ter sido desenvolvido através da revisão de literatura e ter sido objeto de validação por profissionais experientes, deduz-se que a sua aplicação em casos de estudo poderá levar à identificação de *edge cases*, permitindo adaptar a *framework* para corresponder a uma maior amplitude de cenários.

5.2 Trabalho futuro

Em relação ao trabalho que poderá vir a ser realizado no futuro destaca-se:

- Implementação da *framework* em múltiplos casos de estudo para identificar *edge cases*, numa ótima de melhoria contínua do artefacto.
- Aprofundar o estudo de tecnologias IoT associadas à camada de rede, identificando possíveis interferências ou limitações que possam existir em ambiente industrial e, assim, expandir o conjunto de recomendações para a referida camada.
- Alargar a seleção tecnológica às restantes camadas que podem caracterizar uma arquitetura IoT.

Bibliografia

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347–2376.

Almazaydeh, L., Al-Otoon, K., Al-Dmour, A. & Elleithy, K. M. (2016). A panoramic study of fall detection technologies.

AVSystem. (2019). *Top sensor types used in iot*. https://www.avsystem.com/blog/iot-sensors-iot-actuators/

Banaitiene, N. & Banaitis, A. (2012). Risk management in construction projects. *Risk Management–Current Issues and Challenges. In N. Banaitiene (Ed.), Risk Management–Current Issues and Challenges*, 429–448.

Boyes, H., Hallaq, B., Cunningham, J. & Watson, T. (2018). The industrial internet of things (iiot): An analysis framework. *Computers in Industry*, *101*, 1–12.

Britannica, T. E. o. E. (2019). *Industrial revolution*. https://www.britannica.com/event/Industrial-Revolution

Canadian Centre of Occupational Health and Safety. (2020). *Hazard and risk : Osh answers*. https://www.ccohs.ca/oshanswers/hsprograms/hazard_risk.html

CDC. (2015). *The national institute for occupational safety and health (niosh): Hierarchy of controls*. https://www.cdc.gov/niosh/topics/hierarchy/default.html

Chae, S. & Yoshida, T. (2010). Application of rfid technology to prevention of collision accident with heavy equipment. *Automation in construction*, *19*(3), 368–374.

Cheng, C.-W., Leu, S.-S., Lin, C.-C. & Fan, C. (2010). Characteristic analysis of occupational accidents at small construction enterprises. *Safety Science*, *48*(6), 698–707.

Choudhary, G. & Jain, A. (2016). Internet of things: A survey on architecture, technologies, protocols and challenges, Em *2016 international conference on recent advances and innovations in engineering (icraie)*. IEEE.

Collins, R., Zhang, S., Kim, K. & Teizer, J. (2014). Integration of safety risk factors in bim for scaffolding construction, Em *Computing in civil and building engineering (2014)*.

de Morais, C. M., Sadok, D. & Kelner, J. (2019). An iot sensor and scenario survey for data researchers. *Journal of the Brazilian Computer Society*, *25*(1), 4.

Derber, A. (2018). *How these emerging technologies will deliver results soon*. https://www.mro-network.com/technology/how-these-emerging-technologies-will-deliver-results-soon

DIMULESCU, S. & DOBROTĂ, D. (2018). Risk analisys regarding health and safety at work. *Fiability & Durability/Fiabilitate si Durabilitate*, (1).

Ding, J., Nemati, M., Ranaweera, C. & Choi, J. (2020). Iot connectivity technologies and applications: A survey. *arXiv preprint arXiv:2002.12646*.

EU-OSHA. (2018). *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025* (rel. téc.). https://osha.europa.eu/pt/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

FESETE. (2010). *Manual de avaliação de riscos* (rel. téc.). http://fesete.pt/portal/docs/pdf/manual.pdf

Gardner, R. (2003). Overview and characteristics of some occupational exposures and health risks on offshore oil and gas installations. *Annals of Occupational Hygiene*, *47*(3), 201–210.

Gartner. (2019). *Internet of things defined - tech definitions by gartner*. https://www.gartner.com/it-glossary/internet-of-things/

Gerber, A., Kotze, P. & Van der Merwe, A. (2015). Design science research as research approach in doctoral studies.

Gigli, M. & Koo, S. G. (2011). Internet of things: Services and applications categorization. *Adv. Internet of Things*, *1*(2), 27–31.

Gregor, S. & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 337–355.

Guardhat. (2020). *Rasor - lone worker system*. https://www.guardhat.com/hc1-communicator.php

Haj-Bolouri, A. (2015). The notion of users in design science research, Em *38th information systems research seminar in scandinavia (iris 38), oulu, finland, 9-12 august 2015*.

Hassan, Q. F. (2018). An overview of enabling technologies for the internet of things.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design science in information systems research. *MIS Q.*, *28*(1), 75–105. http://dl.acm.org/citation.cfm?id=2017212.2017217

ILO. (2019). *World statistic*. https://www.ilo.org/moscow/areas-of-work/occupational-safety-and-health/WCMS_249278/lang--en/index.htm

Injury Facts. (2018). *Most dangerous industries*. https://injuryfacts.nsc.org/work/industry-incidence-rates/most-dangerous-industries/

IPIECA/OGP. (2006). *Controlling health risks at work: A roadmap to health risk assessment in the oil and gas industry* (rel. téc.). https://www.pdo.co.om/hseforcontractors/Health/Documents/HRAs/HRAIPIECA.pdf

ISO/IEC JTC 1. (2015). *Internet of things (iot) - preliminary report 2014* (rel. téc.). https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

Kanan, R. (2016). Iot devices: The quest for energy security, Em *2016 ieee 59th international midwest symposium on circuits and systems (mwscas)*. IEEE.

Khan, R., Khan, S. U., Zaheer, R. & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges, Em *2012 10th international conference on frontiers of information technology*. IEEE.

Lee, U.-K., Kim, J.-H., Cho, H. & Kang, K.-I. (2009). Development of a mobile safety monitoring system for construction sites. *Automation in Construction*, *18*(3), 258–264.

Li, Y. & Gan, X. L. (2013). Study on the architecture and key technology for internet of things, Em *Advanced materials research*. Trans Tech Publ.

Manson, N. J. (2006). Is operations research really research? *Orion*, *22*(2), 155–180.

Manuele, F. A. Et al. (2008). Prevention through design addressing occupational risks in the design and redesign processes. *Professional Safety*, *53*(10).

Mayton, B., Dublon, G., Palacios, S. & Paradiso, J. A. (2012). Truss: Tracking risk with ubiquitous smart sensing, Em *Sensors, 2012 ieee*. IEEE.

Minerva, R., Biru, A. & Rotondi, D. (2015). Towards a definition of the internet of things (iot). *IEEE Internet Initiative*, *1*, 1–86.

Niven, K. & McLeod, R. (2009). Offshore industry: Management of health hazards in the upstream petroleum industry. *Occupational medicine*, *59*(5), 304–309.

Nyirendaavwil, V., Chinniah, Y. & Agard, B. (2015). Identifying key factors for an occupational health and safety risk estimation tool in small and medium-size enterprises. *IFAC-PapersOnLine*, *48*(3), 541–546.

OH&S. (2018). *Osha announces top 10 violations for fy 2018*. https://ohsonline.com/articles/2018/10/24/osha-announces-top-10-violations-for-fy-2018.aspx

Oppermann, I., Hämäläinen, M. & Iinatti, J. (2005). *Uwb: Theory and applications*. John Wiley & Sons.

OSHA. (2019). *1910.147 - the control of hazardous energy (lockout/tagout)*. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.147

OSHA Education Center. (2018). *Maximum penalties increase in 2018 for osha violations*. https://www.oshaeducationcenter.com/articles/2018-osha-fine-increases/

Ramesh, R., Prabu, M., Magibalan, S. & Senthilkumar, P. (2017). Hazard identification and risk assessment in automotive industry. *International journal of ChemTech research*, *10*(4), 352–358.

Reactec. (2020). *Rasor - lone worker system*. https://www.reactec.com/products_services/rasor

Rout, B. & Sikdar, B. (2017). Hazard identification, risk assessment, and control measures as an effective tool of occupational health assessment of hazardous process

in an iron ore pelletizing industry. *Indian journal of occupational and environmental medicine*, *21*(2), 56.

Safeopedia. (2019a). *What are administrative controls?* https://www.safeopedia.com/definition/5109/administrative-controls

Safeopedia. (2019b). *What are engineering controls?* https://www.safeopedia.com/definition/5070/engineering-controls

Salman, T. & Jain, R. (2019). A survey of protocols and standards for internet of things. *arXiv preprint arXiv:1903.11549*.

Schwab, K. (2016). *The fourth industrial revolution*.

Sommerville, I. & Sawyer, P. (2003). *Requirements engineering: A good practice guide*. John Wiley & Sons, Inc.

Sundmaeker, H., Guillemin, P., Friess, P. & Woelfflé, S. (2010). Vision and challenges for realising the internet of things. *Cluster of European Research Projects on the Internet of Things, European Commision*, *3*(3), 34–36.

Teltonika. (2020). *Gh5200 - autonomous tracker with gnss, gsm and bluetooth*. https://teltonika-sas.com/product/lone-worker-badge-plus/

Thibaud, M., Chi, H., Zhou, W. & Piramuthu, S. (2018). Internet of things (iot) in high-risk environment, health and safety (ehs) industries: A comprehensive review. *Decision Support Systems*, *108*, 79–95.

Thomas, S., Teizer, J. & Reynolds, M. (2011). Smarthat: A battery-free worker safety device employing passive uhf rfid technology, Em *2011 ieee international conference on rfid*. IEEE.

Topmiller, J. L. & Dunn, K. H. (2013). Current strategies for engineering controls in nanomaterial production and downstream handling processes. https://stacks.cdc.gov/view/cdc/21068

Vadimovna, K. E. & Sergeevich, K. M. (2017). Risk-oriented approach to design of the industrial safety system: Problems, solutions. *International Journal of Applied Engineering Research*, *12*(16), 5463–5471.

Wang, W., Lee, K. & Murray, D. (2017). A global generic architecture for the future internet of things. *Service Oriented Computing and Applications*, *11*(3), 329–344.

Wold Economic Forum. (2019). *Accelerating the impact of iot technologies*. https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies

Wu, F., Rüdiger, C. & Yuce, M. (2017). Real-time performance of a self-powered environmental iot sensor network system. *Sensors*, *17*(2), 282.

Wu, T., Wu, F., Redouté, J.-M. & Yuce, M. R. (2017). An autonomous wireless body area network implementation towards iot connected healthcare applications. *Ieee Access*, *5*, 11413–11422.

Apêndice A

Apresentação da *framework* para seleção de tecnologias IoT

Documento apresentado durante a realização das entrevistas tendo em vista a avaliação e validação da *framework* proposta no âmbito da presente dissertação.

Tecnologias IoT na Segurança Industrial

Dissertação de

Mestrado em Gestão de Informação

Fábio Ferreira dos Santos

Orientador: Prof. Dr. Vítor Santos

Instituto Superior de Estatística e Gestão da Informação
Universidade Nova de Lisboa

Acreditações e Certificações

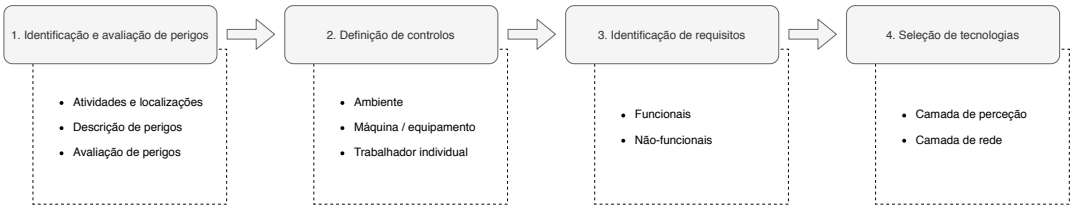
Objetivos da investigação

- Desenvolvimento de uma *framework* que possa ser utilizada por vários setores da indústria;
- A *framework* procura apoiar a seleção de tecnologias IoT da camada de perceção e rede (*);
- As tecnologias selecionadas serão um guia para a aquisição de dispositivos ou sistemas IoT, tendo em vista a melhoria da segurança dos trabalhadores.

(*) Um sistema IoT é constituído por várias camadas, incluindo:
- Camada de perceção: Sensores que efetuam leituras (ex. sensor de temperatura) e atuadores que realizam algum tipo de ação (ex. relé para controlar passagem de corrente elétrica).
- Camada de rede: Mecanismos e protocolos que transmitem dados de/para a camada de perceção.

Framework

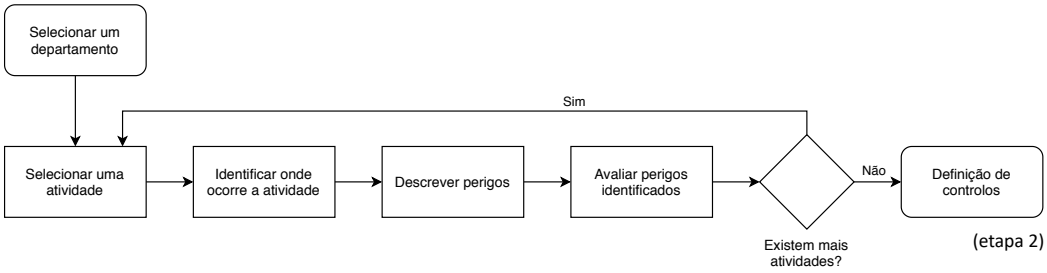
- Constituída por 4 etapas:



- A sua aplicação deverá ficar a cargo de um comité com representantes dos trabalhadores, especialistas em tecnologia e em segurança e higiene no trabalho.

Nota: Os slides seguintes apresentam os fluxogramas e exemplos de *outputs* esperados em cada etapa.

E1. Identificação e avaliação de perigos

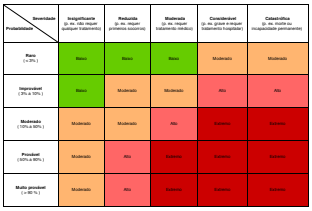


Exemplo de *output* esperado:

Departamento	Atividade	Localização	Perigos			
			Tipo	Causa	Consequência	Risco
Operações	Armazenamento de matéria-prima	Armazém A.1	Químico	Poeira	Problemas respiratórios	M
		Armazém A.2				

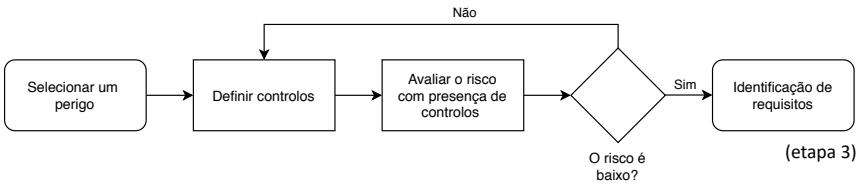
Obtido via uma matriz de avaliação de riscos

anexo 1



Tipos: Geográfico, Físico, Químico, Biológico, Ergonómico e Psicossocial

E2. Definição de controlos



(etapa 3)

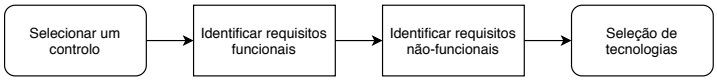
Exemplo de *output* esperado:

Perigos				Controlos			
Tipo	Causa	Consequência	Risco	Âmbito		Descrição	Risco
Químico	Poeira	Problemas respiratórios	M	Ambiente	Armazém 1 Armazém 2	Monitorização de níveis de poeira na área de trabalho	B
				Equipamento	Silo 1 Silo 2 Silo 3	Sistema de alarme sonoro e visual instalado junto aos equipamentos	
				Trabalhador	Departamento de operações	Dispositivo de leitura de níveis de poeira com alarme vibratório	

Existem três âmbitos possíveis

Âmbito da aplicação	Exemplos
Ambiente	- Monitorização de níveis de ruído; - Controlos de temperatura; - Controlos de níveis de gases ou poeiras.
Máquinas / Equipamentos	- Sistemas de anti-colisão; - Sistemas de corte de energia; - Deteção de excesso de velocidade.
Trabalhador individual	- Monitorização de posicionamento; - Monitorização de frequência cardíaca; - Deteção de ausência de movimento.

E3. Identificação de requisitos



(etapa 4)

Exemplos de requisitos:

Tipo	Exemplos de requisitos
Funcional	- Alarmes visuais ou sonoros; - Comunicação de voz; - Deteção de quedas; - Deteção de substâncias químicas; - Deteção da presença de equipamentos ou pessoas; - Despoletar alarmes manuais de emergência; - Monitorização de posicionamento; - Monitorização de movimento; - Monitorização de sinais vitais; - Medição de forças e/ou velocidades; - Monitorização de alterações acústicas; - Monitorização de sinais vitais; - Monitorização de temperatura, luminosidade, pressão atmosférica ou humidade; - Prevenção de colisões; - Prevenção de eletrocussão.
Não-funcional	- Ambiente indoor ou outdoor; - Cobertura elevada, média ou reduzida; - Mobilidade elevada ou reduzida/inexistente; - Identificação do dispositivo de IoT.

E4. Seleção de tecnologias

- Recomendações para a camada de perceção:

- **Alarmes visuais ou sonoros:** Relés para controlar o estado dos alarmes.
- **Deteção de quedas:** Acelerómetros e giroscópios no caso de dispositivos individuais destinados a trabalhadores; Câmeras para alimentarem algoritmos de deteção de quedas.
- **Deteção de substâncias químicas e gases:** Sensores químicos específicos a cada substância. Os mais comuns são sensores de dióxido de carbono, monóxido de carbono, hidrogénio, óxido de nitrogénio, oxigénio, ozono, poluição do ar. A deteção de fumo originado por focos de chamas pode ser possível através de sensores óticos (fotoelétrico) ou por ionização.
- **Deteção de presença de equipamentos ou pessoas:** Além das tecnologias de monitorização de posicionamento, podem ser utilizadas etiquetas RFID e NFC, câmeras térmicas.
- **Despoletar alarmes manuais de emergência:** Instalação de uma interface no dispositivo IoT que permita aos trabalhadores pressionarem botões para gerarem determinados tipos de alarmes ou funcionalidade (p. ex. abertura de um canal de voz com terceiros).
- **Monitorização de posicionamento:** A nível *indoor* podem ser utilizadas tecnologias como UWB, Wi-Fi, Blueetooth, etiquetas RFID; enquanto que *outdoor*, as tecnologias mais indicadas são GPS e UWB.
- **Monitorização de sinais vitais:** Sensores para medição de frequência cardíaca e respiratória.
- **Monitorização de níveis acústicos:** Microfones e sensores piezoelétricos.
- **Identificação de dispositivos IoT**: RFID, NFC, QR codes e códigos de barras.
- **Prevenção de colisões:** RFID, sensores de infravermelhos e câmeras. Alternativamente podem ser utilizadas as tecnologias de monitorização de posicionamento para determinar distâncias de risco.
- **Prevenção de eletrocussão:** Sensores elétricos para verificar a presença de energia elétrica e relés para controlar a passagem da corrente elétrica.

E4. Seleção de tecnologias

- Recomendações para a camada de rede:

Requisitos		**Recomendações**
Ambiente	*Indoor*	Wi-Fi, Bluetooth, UWB
	Outdoor	LTE, 5G, UWB
Cobertura	Elevada	LTE, 5G
	Média	Wi-Fi, LoRA, LTE, 5G, NB-IoT, UWB, Sigfox
	Reduzida	Bluetooth, Wi-Fi, UWB, ZigBee
Mobilidade	Elevada	LTE, 5G
	Reduzida	Bluetooth, Wi-Fi, UWB, ZigBee
Comunicação de voz		LTE, 5G

Questões

- Considera que a *framework* apresentada é útil?
- Concorda com a *framework*?
- Quais são as melhorias que propõe?

Obrigado pela colaboração!

Address: Campus de Campolide, 1070-312 Lisboa, Portugal
Phone: +351 213 828 610 Fax: +351 213 828 611

Acreditações e Certificações

Instituto Superior de Estatística e Gestão da Informação
Universidade Nova de Lisboa

Anexo 1 – Matriz de avaliação de riscos

Severidade / Probabiidade	**Insignificante** (p. ex. não requer qualquer tratamento)	**Reduzida** (p. ex. requer primeiros socorros)	**Moderada** (p. ex. requer tratamento médico)	**Considerável** (p. ex. grave e requer tratamento hospitalar)	**Catastrófica** (p. ex. morte ou incapacidade permanente)
Raro (< 3%)	Baixo	Baixo	Baixo	Moderado	Moderado
Improvável (3% a 10%)	Baixo	Moderado	Moderado	Alto	Alto
Moderado (10% a 50%)	Moderado	Moderado	Alto	Extremo	Extremo
Provável (50% a 90%)	Moderado	Alto	Extremo	Extremo	Extremo
Muito provável (> 90 %)	Moderado	Alto	Extremo	Extremo	Extremo

Apêndice B

Entrevistas

Transcrição das entrevistas realizadas no âmbito da avaliação e validação da *framework* proposta no âmbito da presente dissertação.

B.1 Especialistas em segurança industrial

B.1.1 Especialista #1

Nome: Bruno Domingues

Breve biografia: Formado em Gestão Industrial e Profissional de Segurança do Trabalho. Possui experiência relevante na Indústria Siderúrgica, tendo ocupado posições de Técnico de Segurança Ocupacional em empresas de grande dimensão como a Votorantim Siderurgia e ArcelorMittal.

Q1. Considera que a *framework* apresentada é útil?
Sim, pareceu-me bastante útil.

Q2. Concorda com a *framework*?
Sim, concordo com a estrutura apresentada.

Q3. Quais são as melhorias que propõe?
Acrescentaria além dos gases descritos na secção "Seleção de tecnologias > Detecção de substâncias químicas e gases", o gás H_2S, muito comum em espaços confinados devido à decomposição de substâncias orgânicas, etc. Os aparelhos que detectam gases utilizam um sistema destinado à deteção de 4 ou mais gases como no exemplo do site: https://br.msasafety.com/pn/10127163C

B.1.2 Especialista #2

Nome: Anderson Taschin

Breve biografia: Formado em Engenharia Ambiental e Pós-graduado em Engenharia de Segurança do Trabalho. Ao longo dos últimos 15 anos, ocupou várias posições de Técnico e Engenheiro de Segurança e Higiene no Trabalho em várias empresas multinacionais como a Ferrero, Rockwell Automation e ABB.

Q1. Considera que a *framework* apresentada é útil?
A *framework* apresentada é útil para o processo de segurança.

Q2. Concorda com a *framework*?
Sim, concordo.

Q3. Quais são as melhorias que propõe?
A estrutura proposta funciona, mas o ser humano é complicado e podem existir brechas resultantes da aplicação da *framework*. Para as prevenir, deve-se aumentar o número de controlos para determinados riscos críticos de modo a que diminua a probabilidade de ocorrerem. Em relação a riscos mais baixos é aceitável ter menos controlos.

B.2 Especialistas em IoT

B.2.1 Especialista #1

Nome: Henrique S. Mamede

Breve biografia: Professor auxiliar na Universidade Aberta e coordenador do Mestrado em Informação e Sistemas Empresariais. Doutorado em Sistemas e Tecnologias de Informação pela Universidade do Minho e Mestre em Informática pela Universidade de Lisboa. Consultor em Sistemas e Arquiteturas de Informação, Aplicacionais e Tecnológicas.

Q1. Considera que a *framework* apresentada é útil?
Sem qualquer dúvida, a *framework* que propõe, para além de inovadora, é muito útil particularmente nos ambientes industriais.

Q2. Concorda com a *framework*?
Concordo. A mesma parece completa, cobre os aspetos fundamentais do ambiente industrial e mostra como se aplica, ou seja, não se limita a ser uma proposta meramente teórica, deixando à interpretação individual a aplicação da mesma e os outputs que se obtêm.

Q3. Quais são as melhorias que propõe?

As melhorias que proponho, após reflexão, estão mais focadas no nível das recomendações para a camada de rede. Sugiro que atualize as tecnologias que refere, pois não são utilizadas em ambientes mais recentes de IoT. Assim, sugiro que recomende, para além de Wi-Fi, LoRaWAN ou 5G. Neste último caso, tem muito a ver com os serviços 5G que eventualmente estejam contratados com o operador.

Redes tipo SigFox ou Zigbee estão obsoletas. O Bluetooth não é alternativa, nem em situações de muita proximidade. As redes LTE acabaram, na prática, por não saírem do conceito em papel.

B.2.2 Especialista #2

Nome: António Jordão

Breve biografia: Mestre em Engenharia Biomédia pela Universidade Nova de Lisboa, fez investigação na área de processamento de sinais e desenvolvimento de sistemas embarcados e saúde móvel. Com uma década de experiência em desenvolvimento de software e aplicações móveis, é atualmente *Tech Lead* na Fujitsu com principal foco na área de IoT e desenvolve projetos que envolvem sensorização e recolha de dados para fins analíticos e de inteligência artificial.

Q1. Considera que a *framework* apresentada é útil?

Sim será útil, está bastante simplificada e aponta todos os pontos relevantes. Utilizando a *framework*, o levantamento das necessidades poderá ser mais adequado poupando tempo e dinheiro, e proporcionando segurança aos trabalhadores.

Q2. Concorda com a *framework*?

Numa primeira análise sim, parece contemplar todos os pontos de interesse para a seleção da tecnologia certa.

Q3. Quais são as melhorias que propõe?

Tentaria complementar o ponto da seleção das tecnologias, pois podemos ter vários tipos de tecnologia a resolver o mesmo problema. O mais importante é perceber em que ambiente estas serão usadas de forma a garantir uma melhor relação qualidade-custo oriunda da sua utilização.

Nas recomendações já temos para a camada de rede a divisão entre *indoor* e *outdoor*, mas muitas vezes o mais importante é uma análise do ambiente em termos de materiais e interferências externas, como por exemplo paredes de betão que podem funcionar como gaiola de Faraday ou motores elétricos que possam criar campos magnéticos que interfiram com as ligações.